

RE: Publishing Nimda Logs

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2002-05/0057.html>

From: Benjamin Tomhave (falcon@cybersecret.com)

Date: 05/08/02

From: "Benjamin Tomhave" <falcon@cybersecret.com>

To: <incidents@securityfocus.com>

Date: Wed, 8 May 2002 10:15:18 -0600

Whoa, whoa, whoa....having worked for an ISP in recent history, I can honestly tell you that most knowledgeable techs are just as frustrated with infected end-users as everyone else, so sending single email messages with each SYN, etc., is a BAD IDEA. You're basically saying that you want to further prevent these people from doing their jobs altogether, or to start ignoring your messages altogether, because some end-users are universally ignorant and negligent.

Instead, there are few things which ISPs can and should be doing with this matter. First, acceptable usage policies have to be updated to current contexts and continuously presented to customers as a reminder of their responsibility. One of the key portions of updated policies should be verbatim along the lines of "If your system(s) become(s) infected with a worm, virus, trojan, or has become compromised by attackers and used for other purposes, ISP reserves the right to suspend and/or terminate your service without prior notice." Then the ISP can legally blackhole the offenders. Second, ISPs should not be allowing inbound traffic to accounts that aren't paying for it. In other words, firewall off those residential (and problematic) users! They aren't generally paying for business class service, so why give it away? Though this won't help defend against customers who are already compromised, it should go a long way toward minimize the compromise of residential (and perhaps even "basic business") customers in the future. Third, as much as it sucks, ISPs *must* be willing to discontinue service to problematic customers, despite the desire to have that revenue stream intact. It's simply a matter of acting responsibly. Along with this, if a customer has to be terminated for causes stemming from compromise, negligence, etc., then local, state and federal authorities (depending on scale) should be notified of the problem and lawyers should probably be brought in, even if only as a precautionary measure. The contrapositive of this is to have fully open, completely unregulated Internet service, which is a trend we are getting away from because of the record for abuse.

On the idea about listing IPs, logs, etc. — though I think this is an ok idea, I agree with the comment regarding SMTP relays and the effectiveness of ORBS and co. Though it would be very cool to setup a system similar to

SecurityFocus Incidents: RE: Publishing Nimda Logs

the RBL lists and be able to automate routing blackhole lists, I can see this information being abused in a number of ways. Furthermore, one of the key frustration with the SMTP RBLs is that the lists often are not updated and re-evaluated quickly enough, if at all. In fact, I'm aware of some rogue RBLs that have blackholed entire ISPs (Qwest, Sprintlink, BellSouth, etc.) because they are "known spam hosters" — which is hardly fair to those customers who are not open relays, but get blackholed anyway. Thank goodness these people are the minority, but regardless, it doesn't make me want to push use of RBL lists. The other thing comes down to asking who among us wants to donate the time to maintain a routing blackhole list for this sort of thing? If you're already a sysadmin/netadmin/infosec for your company, you likely don't have a lot of time to chance these things down, right? So, that kind of kills things.

Just remember: Silver was a horse, not a bullet. :)

cheers,

—ben

-----Original Message-----

From: root@securityfocus.com [mailto:root@securityfocus.com] On Behalf Of E

Sent: Wednesday, May 08, 2002 5:50 AM

To: incidents@securityfocus.com

Subject: Re: Publishing Nimda Logs

I have struggled with this problem for months. My ISP has a large number of broadband users, and these people are still infected with nimda. I tried for weeks to get them to do something about it. I even started offering them technical suggestions on ways to prevent it. The end result was absolutely nothing. They obviously do not give a damn about it, and this goes for many other ISP's and organisations. The people who are infected with nimda are being criminally negligent. They are allowing their machines to reinfect others. (Personally I also think Microsoft is criminally negligent for releasing the bogus webserver and OS in the first place).

The last resort that I can think of is mailing your nimda logs to the ISP, and yes, I mean every single SYN that comes in should go to them in a separate email. Then perhaps their tech / security people will

RE: Publishing Nimda Logs

SecurityFocus Incidents: RE: Publishing Nimda Logs

start to realise what a complete annoyance this worm is.

Publishing the IP's will achieve nothing. Each infected person needs to be notified that he/she is infected.

Many are just broadband users in dynamic ip pools, who probably are not aware

of the problem anyway.

The bets are most network admins dont care about it, perhaps dont even know their users are infected.

Serious lessons should be learned here. This is the kind of thing that happens

when you dress up an OS

designed for secretaries as a webserver / multiuser OS, and put it in the hands

of millions of

ignorant users. I am shocked that MS is not being held accountable for this (and the multide of

other worms in the past couple of years).

When are people going to realise that a corporation who puts its OS into the

homes of millions of people,

bears some responsibility for the damage, cost, annoyance and above all wasted

time caused by poor

standards.

Deus, Attonbitus" wrote:

> -----BEGIN PGP SIGNED MESSAGE-----

> Hash: SHA1

>

> *It is truly sad that so many people are still infected with Nimda. There is a company with my corporate ISP that I have notified 3 times now that they are attacking other systems. It seems they can't figure out how not to install Win2k/IIS5.0 while connected to the net. The sad thing is that*

> *this is a computer company.*

>

> *I have seen a site where people have published the IP of the offending boxes for stuff like Nimda and CR. I am thinking about doing the same thing so that people can either use that information to block the IP's or*

> *to do whatever they want for that matter.*

>

> *I'm curious to see how other feel about this. Is it:*

>

> *1) Recommended. Go for it and publish the IP's and let the "Gods of IP" sort out the damage.*

> *2) A Bad Thing. These are innocent victims, and you will just have them*

SecurityFocus Incidents: RE: Publishing Nimda Logs

be

> *attacked by evil people.*

> *3) Boring. Who cares? It's Nimda, and an everyday part of life. Deal*

with

> *it and ignore the logs.*

>

> *If "1," then I was thinking of going with a "Hall of Shame" and*

providing

> *ARIN look ups, contacts, and the whole bit. I could even allow other*

> *people to post logs there and stuff like that...*

>

> *Input appreciated.*

>

> *AD*

>

> -----BEGIN PGP SIGNATURE-----

> *Version: PGP 7.1*

>

> *iQA/AwUBPNgHPIhsmYD15h5gEQLsWACZASlSx6Wew0YfTHAzIHxotQYAdkAAoIoV*

> *VSob5Hcw7X9DDzDxNUzXftdm*

> *=Xv5m*

> -----END PGP SIGNATURE-----

>

>

--

> This list is provided by the SecurityFocus ARIS analyzer service.

> For more information on this free incident handling, management

> and tracking system please see: <http://aris.securityfocus.com>

This list is provided by the SecurityFocus ARIS analyzer service. For more information on this free incident handling, management and tracking system please see: <http://aris.securityfocus.com>

This list is provided by the SecurityFocus ARIS analyzer service. For more information on this free incident handling, management and tracking system please see: <http://aris.securityfocus.com>

- **Previous message:** Richard.Smith@predictive.com: "Re: Publishing Nimda Logs"
- **In reply to:** [E: "Re: Publishing Nimda Logs"](#)
- **Next in thread:** [John Kristoff: "Re: Publishing Nimda Logs"](#)
- **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)