

Re: increase in spam and what to do about it

Re: increase in spam and what to do about it

Source: <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2006-11/msg01614.html>

- *From:* bill@xxxxxxxxxxx (Bill Gunshannon)
 - *Date:* 22 Nov 2006 18:56:07 GMT
-

In article <1164209725.524594.74340@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>, davidc@xxxxxxxxxxx writes:

Bill Gunshannon wrote:

In article
<1164168707.352713.194240@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>, davidc@xxxxxxxxxxx writes:

What I would like to do is have a DNS server that does an RBL check for every host requesting an MX lookup. If it's on the RBL, return a 127.0.0.1 as the preferred MTA! Save me a lot of traffic.

The problem with that is that machines can become infected much faster than the RBL's can learn of them.

I know, but it would still save me a lot of traffic.

Not to mention all the legitimate emails that your server will reject because your potential customer is using an ISP that happens to get itself "blacklisted".

This is not a technical problem it is a social problem. There are no technical solutions to social problems. It takes a social solution.

There are technical solutions that can help quite a bit.

Re: increase in spam and what to do about it

As fast as you can come up with a technical solution the spammers will come up with a way around it. It has to be stopped at the source, and there is no technical way of doing that. There is a social way.

Unfortunately, that would require a technical solution from Microsoft that would harden their Windows platform, as the vast majority of zombies are Billy-boxes. ISP's could be more proactive in identification and isolation of zombies, but they don't have the guts to do it (even if they just blocked port 25, that would solve a lot).

Both of these can be fixed with my social solution. Right now there is no incentive for any ISP to fix any of this while there are many incentives not to.

The big social problem is that just enough people BUY from these scams to make them profitable enough (even if only the gambling sense – I almost won all my money back, so just one more spam run and I should finally hit to big one!).

Actually, I saw an interview on the news with a commercial spammer. he said all it took was .1% return for him to make a profit. Of course, that leaves the other 99.9% (us) having to deal with it. It will always be profitable for the spammer, which is why it must be stopped at the source. Right now it costs them nothing to send out 100,000,000 emails. The only solution is to remove that conduit so they can't send them.

That solution
is for email to only be exchanged between consenting sysadmins.
And when someone violates the consent agreement, you cut them off.

The problem is creating the "trust relationships" in the first place, when you have a userbase which is orders of magnitude larger than the original UUCP network.

Personally, I doubt that the useful base of legitimate mailhosts is "orders of magnitude" larger. The actual number of users has little if any effect on the "trust relationships". It is the admins of the mailhosts themselves that establish the trust. Much like what is done Usenet News today.

Re: increase in spam and what to do about it

And unless you smart-hosted, generating paths to nodes was rather pain-staking – but someone had to do it so you could figure out the "trusted" path.

But that would be much easier to do today as basically anyone can talk to anyone, from the technical standpoint. We could have central hubs, like what was done by seismo in the old days, but they would be more of a convenience than a necessity. I am not saying everyone has to have an explicit agreement with everyone else with whom they wish to exchange email. I am saying that there needs to be an explicit agreement drawn up that everyone who wishes to take part must sign (as a legally binding document) in order to exchange mail with anyone in the Email network. Once you join the network, peering is can be left to the individual admins. Again, much like Usenet News, but with a much stricter and enforceable AUP.

When the predominate problem was with "trusted hosts", i.e. most mail running through an ISP's mail servers, the spam wasn't as bad and even RBL's more effective.

If only it were so. While much of the spam coming into my mailserver comes from the proverbial "rogue" PC I get a considerable amount from ISP's who really have no problem with spammers. The profit currently outweighs the potential cost.

Even early in the battle with Walt Rines and Sanford Wallace, there was substantial blackholing of the entire AGIS backbone (a very strong social statement) against spam and their support to two of the worst known offenders.

And who paid the price? What effect did this have on AGIS legitimate users?

The problem is today, you can't take that kind of risk with 99.9% of your customers getting their e-mail dropped because that 0.1% caused you to lose your trust relationships and got you blacklisted.

Sorry, ISP's don't see it that way. It's all about the money. As long as there is money in spam they will support the 0.1%. There are some major ISP's that show up on RBL's and do nothing to get back off them. Why? Because there are still lots of email servers that don't use RBL's or can't because of the very reason you cite above. That leaves lots of potential targets

Re: increase in spam and what to do about it

Re: increase in spam and what to do about it

and, anyway, as long as the spammers are willing to pay for the connection and service, why would the ISP care if the email ever gets delivered?

That doesn't mean they can't identify and isolate that 0.1%, but the problem is getting harder and more frequently occurring than ever before (i.e. the new SpamThru trojan).

Which comes back to why it has to be stopped at the point of origin. And we won't even get into the load on the whole infrastructure of rejecting at the destination rather than stopping it at the source.

Being as every schmuck on the INTERNET should not be sending Email from their desktop PC this system is not as complex as you might think.

Which is why ISP's should route all port 25 through their own mail servers so they can help isolate the culprits rather than let them loose. But because of potential social repercussions, they don't/can't do that.

And why is that? Because right now, under the current system there is no penalty for allowing it and a perceived penalty for stopping it.

Social solutions are can only be part of the solution. The technical ability to zombie a box has got to be eliminated/reduced as well. That is Gates true legacy – a world full of insecure systems subjecting everyone else to spam, DDoS attacks, fraud, identify theft, and more.

I don't agree on two points. I don't believe that "The technical ability to zombie a box has got to be eliminated/reduced". And, moreover, I don't believe that "The technical ability to zombie a box can be eliminated/reduced".

I think the big problem with people accepting my idea up to this point is more a matter of them thinking it is an all or nothing deal. That's not true. This can easily be phased in over time. Once you start to establish your "trusted mailhosts" you can continue to accept email from the open INTERNET or, you can choose much more draconian filter methods or, you can just stop accepting mail from outside the system.

Re: increase in spam and what to do about it

Re: increase in spam and what to do about it

All of it is at the choice of the sysadmin (with or without the approval of his userbase.) hey, I have no problem with spammers sending their junk to all my neighbors. Who knows, maybe they comprise the .1% who actually want it. I just want the utility of email that I had in the original Usenet days back. There will be a market for mail services that offer spam free accounts (like gmail, only without the ability to send spam) they will be different and definitely not anonymous, but then, with privilege comes responsibility. In any event, something has to be done or email will become useless for real communications.

bill

--

Bill Gunshannon | de-moc-ra-cy (di mok' ra see) n. Three wolves
bill@xxxxxxxxxxxxxxxx | and a sheep voting on what's for dinner.
University of Scranton |
Scranton, Pennsylvania | #include <std.disclaimer.h>

.