

Re: OT: GMail and Spam

Source: <http://sci.tech-archive.net/Archive/sci.space.history/2005-03/1977.html>

From: Craig Fink (WeBeGood_at_GMail.Com)

Date: 03/22/05

Date: Tue, 22 Mar 2005 14:30:03 GMT

On Tue, 22 Mar 2005 05:54:30 +0000, Henry Spencer wrote:

> In article <pan.2005.03.21.02.50.50.707644@GMail.Com>, Craig Fink
> <WeBeGood@GMail.Com> wrote:
>>> ...So the spammers aren't getting the bills, and they have an
>>> essentially unlimited supply of CPU cycles at their disposal.
>>
>>I wouldn't call it unlimited, not yet anyway. Depending on the algorithm
>>used, the amount of CPU time could be greatly vary. So if it takes each
>>machine 1000, 10000 or even 1,000,000 times the CPU time for each
>>e-mail, the hijacked machine can only send out 1/1000th, 1/10000th or
>>1/1,000,000th the amount of spam.
>
> Remember that machine speeds vary greatly -- not all operating systems
> require you to constantly upgrade your hardware just to keep up with the
> software bloat -- and that there are machines which legitimately have
> cause to send lots of mail, e.g. mailing-list hubs. I'm very skeptical
> of being able to pick a level of effort which will not be prohibitive
> for legitimate users and yet will impose serious burdens on spammers.
> (There are so many zombie machines out there that they can easily pick
> the best and fastest, bearing in mind that there's a strong correlation
> between vulnerability and the need for constant hardware upgrades...)

The difference between the vast majority of legitimate users and legal and illegal spammers is the sheer volume of e-mail sent out. There is and always will be some cost associated to send an e-mail or spam. Currently, it's extremely very small, increasing the cost (money or time) reduces profitability. Basic economics.

Even a mailing-list hub knows how many e-mails it's going to send out on a regular bases. If it's hijacked they're going to want to know about it, same for a company, or even an individual. A thief spammer really doesn't want it's zombie to realize it's a zombie, that way they can use it longer. They're just thieves, who what to steal resources for as long as possible.

People pay attention when there is money involve, it's human nature. Rate limiting yourself (\$\$ in an e-mail checking account that should have a

zero \$\$ rate loss) allows you to decide what e-mail rate you want. The e-mail is still free, unless your account is hijacked, then you've just paid for some spammer's spam, and for your own lack of security. Plus, when your e-mail sending privileges comes quickly to a screeching halt, your going to know your systems has been compromised much sooner.

It's a self determined rate limit.

I think the real intent of the concept isn't wrt zombies (thieves), but legitimate spammers who follow the rules and laws. To increase the cost to them slightly. Which reduces their profitability and therefore the amount and type of spam they send out.

If a legitimate spammer makes a profit by receiving just one reply in 100,000 e-mails, he can afford to send billions and billions of pieces of spam. Increase his costs slightly and profitability goes down, and he's going to get smarter about sending out spam because money and profitability are involved.

> *Too many of the folks who invent such schemes never seem to think hard*
> *about possible problems or countermeasures; they assume an idealized*
> *world in which all legitimate mail users are similar and the spammers*
> *are not allowed to react intelligently.*

Actually in the article, they say the \$\$ concept is complex and may be costly.

But, for the most part spamming is about money and profitability. So, inevitably the solution to reducing the exponential growth of spam is going to have to involve money and profitability, of both the legal and illegal spammers.

>>...*When the user of the hijacked machine notices that his machine seems*
>>*to be moving at a crawl...*
>
> *As I understand it, there are already zombie control programs which stop*
> *the unauthorized activity the instant the mouse moves or a key is*
> *pressed, and resume only when all is quiet. The user never notices*
> *anything wrong.*

Yeah, doesn't what his zombie to be discovered, a thief in the night.

>>*or his e-mail bill is*
>>*growing rather fast, or he ran out of "pay as you go money", he's more*
>>*likely to fix his machine.*
>
> *A hit in the pocketbook will get people's attention... but they need to*
> *have something they can usefully do about it. That's actually not a*
> *trivial problem for independent Windows users (that is, people without*
> *savvy tech-support staff handy) these days. Install the latest upgrade?*
> *That's the one that breaks half the software, right?*

That's all part of the price someone pays for buying a computer and connecting to the Internet.

>>One dollars in your e-mail check book account would allow you to send
>>unlimited e-mails, but limit the rate to 100 e-mails (a penny per
>>e-mail) at any one time. After that you can't write any more e-mail
>>checks, or send any more e-mail, until some of those written checks
>>expire without being cashed (cashed check = spam).

>
> There will be quite a few people who'll need more than that, especially
> people who use email for *work* with substantial groups of
> correspondents, and simply cannot have their email arbitrarily
> interrupted. The spammers can and will select well-funded zombies.

Hummm, your system is compromised, ignore it and keep on working? I guess a few people might do that.

> Yes, there are conceivable fixes for this sort of thing, but the
> conceptual simplicity is quickly lost as complication after complication
> is applied to try to rescue a fundamentally over-simplistic concept.

>
>>Also, to
>>get the mail through requires a round trip and valid addresses at both
>>ends, not just a mail server willing to accept and send.
>
> I'm not quite sure what you're saying here, but I'd be willing to bet
> the zombie legions won't have any trouble pretending to be legitimate.

Have you ever replied to the sender of some spam to ask them why they are sending you the spam, or to tell them their computer has been hijacked. If you have, the e-mail most likely bounced back to you. In the US, our Congress passed a law requiring spammers to have valid return addresses. Yet, the spam without valid addresses continues to grow.

A form of authentication, did the person really send you an e-mail. Currently, all the spammer needs is the account name and a password to send you something from some unwilling participants account. The unwilling participant never sees anything to indicate that they're account has been hijacked. The spammer really doesn't want the unwilling participant to know that their account has been hijacked, so he modifies the header and there is no valid return address. The sooner an unwilling participant finds out his computer is compromised the better.

>>The Scientific American article is a good one, and really talks about a
>>multifaceted anti-spam effort for a spam free future :-J, not a silver
>>bullet. I just found these two of the more interesting concepts.

>
> I fear that a multifaceted approach which includes concepts like those
> is not likely to be sufficiently well-thought-out to do the job.

sci.space.history: Re: OT: GMail and Spam

The article talks about legislation, sender id (anti-spoofing) safe-sender list, reputation service, machine learning filters, proof systems.

I still think it's a good article....and....the Spam War continues.

--

Craig Fink
Courtesy E-Mail Welcome @ WeBeGood@GMail.Com