

Re: Cyberterrorism [was: Re: NSA wiretap, Friday night]

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2006-09/msg00027.html>

- *From:* responder <no@xxxxxxxxxxxxxx>
 - *Date:* Thu, 07 Sep 2006 18:08:06 -0400
-

Kevin the Drummer wrote:

responder <no@xxxxxxxxxxxxxx> wrote:

Kevin the Drummer wrote:
[snip]

So, what can WE do [to improve cyber security]?

Whether any particular illicit activity is most correctly called criminal or terrorist

I suppose that there is overlap in the protection schemes between those two classes of attackers.

A botnet set up by a criminal can be sold to a terrorist. The original intent was to limit the growth of botnets. If people see that this is important to do for any reason, they will be more inclined to accept the uniform rule to disconnect compromised machines.

1. Keep your own systems in order, updated and secure so you don't become part of the problem.

Of course! Gotta worry about the other folks tho. You cover that below some.

2. Use a (firewall) log aggregation service

Yup.

Re: Cyberterrorism [was: Re: NSA wiretap, Friday night]

3. Advocate (gently) for computer and network security, to people you know personally, especially if they are doing unsafe things.

I already do.

4. ... I think that there needs to be a generally accepted and acceptable standard that if a connected computer is compromised, it should be disconnected.

That would need to be somehow seen as a benefit to the end user. Before the explosion in spam having someone else filter one's email would have been wholly unacceptable. Now it's seen as an absolute need. Having one's computer disconnected needs to be seen as a need and managed well enough so as to provide a good way back to a connected usable system.

Yes. There is work to be done in educating and motivating people in the need for this. It does need to be widely accepted and supported. It is the most non-disruptive and non-punitive plan I could outline. It can be improved, and your comments are constructive.

For myself, I can see a real benefit just in preventing criminal or terrorist activity. And while the plan should be non-disruptive to the legitimate users, it should absolutely be as disruptive as possible to the bot-meisters.

This benefit doesn't have a price tag; it cannot be easily quantified. We don't yet have a clear example like the oft repeated example of "9/11". And we really shouldn't wait for one or hope for one.

Perhaps this could be tied in to some other coupled benefit such as help with peoples' compromised machines, as you suggested below. Maybe someone else could comment on this

In order for such a system to be uniformly applied in a fundamentally non-punitive and non-disruptive way, the enforcer role must be essentially separated from from the discretion of the ISP.

I *think* I agree with that. I wonder if it's really needed tho. Wouldn't someone move from one ISP to another if it was really bad at their original ISP?

I think that may actually be one of the best arguments in favor of the need for a statutory requirement. Specifically *if* the requirement and the implementation is is uniform and identical at all ISP's, there would

Re: Cyberterrorism [was: Re: NSA wiretap, Friday night]

be little or no motivation to switch providers. It shouldn't be bad at any ISP, and the procedures and the proxy servers at any ISP should be functionally identical. That's the plan anyway. This exact question would surely be a central concern to any ISP and would need to be carefully addressed. One original thought was that a coordinating authority would have names of users who were recently referred, and could check all names requesting new service from other ISP's in the area. If the user is switching providers to avoid cleaning the machine, the new provider would be required to do exactly the same thing as the original provider was required to do. This is not draconian. It is simply the enforcement mechanism needed to provide uniform application of the rule, and to protect ISP's from exactly this kind of exposure. The need for uniformity is why I think that it needs to be statutory. I would think it would be welcomed by ISP's because they would not be the "bad guy" in disconnecting a compromised user, but only obeying the terms of a statute and community standard. Perhaps that's an error.

I wonder if someone could subscribe to an as of yet non-existent service that would inspect their traffic for troubles and do the shutdown?

I'm not sure I see a clear benefit in that. As I see it, the shutdown is mostly symbolic, with a purpose to be sure that the user got the message that his box is compromised and needs to be cleaned. If the user says he needs the connection open, the ISP can open it through the proxy server. That box would be set to filter mal traffic from the user to protect other users. It might not pass all the traffic the user wants (or thinks he wants), and it might be marginally slower. Aside from that, it would be a fully functional connection.

I considered a suggestion to eliminate the actual disconnection in favor of simply switching the connection to the proxy, sending an automated e-mail and placing a banner and hyper-link at the top of all web pages. I don't think that would be as effective as requiring the customer to specifically ask for the proxy connection. There could be other issues with an automatic switch-over. I think the manual method is better.

At one time I thought about non-intrusively filtering all traffic for UDP spam, because it's almost impossible to control that any other way. But it would really require software running on multiple machines at all access points. I couldn't rigorously support that.

I wonder if there is some way, sort of like your proxy idea, to have a brown-out of the connection?

This would be a little bit browned out, but not much hopefully. I think it is important for the user to acknowledge the problem and agree to the need for remediation. The server could host some simple helps for self

Re: Cyberterrorism [was: Re: NSA wiretap, Friday night]

remediation and where to get outside help. Most ISP's already have such pages posted.

I expect that technical issues would be minimal, initial set up costs relatively low, and initial and ongoing costs to be reimbursed to the government authority

Does it really require government intervention? Can't it be a fee service paid to a 3rd party, or even the original ISP? Considering your original NSA thread, do you really want the gov't involved at all?

For the reasons stated, I think it does. Congress has traditionally stayed away from regulating the internet, and I am glad for that. This is a bit different because it is really a defensive measure to protect all network users from attacks. I don't see a practicable way to do this without statutory requirement. The proceeds of fees would only go towards the most minimal of administrative costs with the bulk being returned to the ISP for their hosting and other costs. In effect they would be getting paid for doing what they are now doing for free.

WRT the warrantless wiretap, that is an abuse of power because it clearly seems, and has been judged to be illegal and unconstitutional in very significant ways. It appears to be a direct affront to the rule of law and to every citizen. I don't necessarily feel comfortable with FISA, for example, but prefer that laws be uniformly and fairly enforced, or else challenged properly, – rather than ignored. We need to have our "leaders" show proper respect for laws that are on the books as well as to the Constitution.

While any authority *might* be abused, I really wonder who might think they would benefit from abuse of of a "mandatory disconnect" statute, while simultaneously being in a position to do so.

It is proper for government to provide for common security needs, particularly when private sector cannot effectively do so. All parts of the work that can be done by the private sector, should be. And that is the plan as I see it.

Detection of compromised machines could be done the same way and by the same people who now do so: namely log aggregation services. Additional or alternate strategies could also be used, but would not seem to be necessary.

Should there be any detection of client machine components to see if they have vulnerabilities? For example, if someone is running a really bad version of IE or Exchange, should the user be alerted by

Re: Cyberterrorism [was: Re: NSA wiretap, Friday night]

Re: Cyberterrorism [was: Re: NSA wiretap, Friday night]

email that their service will be restricted (brown out or disconnect) after some number of minutes or days?

No, I would not think so. The criterion should be that if a connected machine is compromised, it should be disconnected. Nothing more is needed or justified.

A "Standard Operating Procedure" would be developed to specify what actions would happen and when they would happen. This procedure would be drafted with the input of all users and providers. This SOP would then be enforced by the statute. And the statute could authorize a procedure for modification of the SOP.

I can see that it could escalate to the above extent. But, the black-hats are very adaptive and fast. I'm not sure that a statute could keep up. Just imagine how fast Symantec could respond if their were a statute governing what they provide.

Well, nothing says the ISP can't respond fast to any new threat, or in any ways that they would normally deem appropriate. The SOP would only deal with the procedures needed to implement the disconnection and reconnection, and the specification of the proxy server. So as technology changes over months and years, the SOP would be flexible enough to change in that time frame. A coordination authority could have a paid or voluntary board of advisors or such who might or might not meet face to face from time to time or when they thought necessary. They could include representatives from ISP's so it would be responsive to everyone's needs (except of course the bot-meisters.)

The essential elements are: (1) the ISP is notified (as now) of a compromised machine and then notifies the customer and the coordinating authority. The customer's identity would need to be included for the plan to be effective, but that information need not be retained indefinitely or necessarily reported to others. (There could be a "mandatory disconnection" of one day to be assured that the customer did indeed get the message, which could also be waived at the customer's request for reason and with some restrictions.)

(2) The ISP hosts a (paid) proxy server on their premises that is built and maintained as specified in the SOP. When the customer is reconnected (for reason or need or when repaired) his connection is proxied through this server for a (specified) few days. This allows the ISP time to know that the machine is clean, certify this to the CA and resume a normal connection.

The proxy server would be built to some standard to minimize or

Re: Cyberterrorism [was: Re: NSA wiretap, Friday night]

mitigate the transmission of malware vectors by the (previously?) compromised machine(s). And it would allow (limited?) connection for the need or convenience of the customer.

[snip]

What do you think? Is this doable? Is it advisable? Are there other suggestions that are better?

I think that's a starting place. Maybe something like this would make a good research project at a university. Universities would also make a good proving ground, and the ISP (the school) is small enough to be adaptive to such a system while it's in development.

I think a University would be an excellent test-bed. And it would be valuable to have academic input.

Thoughts from other folks?