
From: Vincenzo Iozzo <[REDACTED]>
Sent: Monday, September 26, 2016 11:56 AM
To: Jeffrey E.
Cc: Joi Ito; Danny Hillis; Reid Hoffman
Subject: Re:

Warning: this is likely going to be a long essay, but I think it gives some perspective on the topic.

The short version is:

I was talking to Joi about this the other day - I wouldn't pay too much attention to this, Schneier has a long tradition of dramatizing and misunderstanding things.

That said, buying Cloudflare (it's private) or Akamai stock might be an idea because DDoS attacks are not going away soon and as a trend they will likely increase.

Also to provide some perspective, he links to this: <https://www.verisign.com/assets/report-ddos-trend-Q22016.pdf>
<<https://www.verisign.com/assets/report-ddos-trends-Q22016.pdf>>

If you look at the numbers on page 9 they are an order of magnitude smaller than the attack on a, rather unknown to the general public, cyber security journalist: <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/> <<https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>>

<div style="background-color: rgba(255, 255, 255, 0);">And we are talking average not median..

CloudFlare was able to absorb most of the attack on Krebs' website and they probably brought the website down because he wouldn't be able to pay for the service at that rate anyway. So those numbers there are nowhere close to "probing" the limits as he suggests..

</div>

</div>

The more interesting aspect is that DDoS attacks boil down to two strategies:

- 1) "amplification" attacks - which is a textbook example of the tragedy of the commons
- 2) Force real traffic to happen. This often happens when you compromise a device (that's what a botnet does). In that sense IoT is particularly dangerous

(1) Is a good argument for Danny's idea of building a backup internet. The problem there is that a lot of protocols (DNS, NTP etc etc) have design flaws in that you can generate asymmetric amounts of traffic and force the traffic to go to some other destination. (eg: <https://www.us-cert.gov/ncas/alerts/A13-088A> <<https://www.us-cert.gov/ncas/alerts/TA13-088A>>)

In a lot of cases people leave around the internet vulnerable servers and those are used for these types of attacks (hence the tragedy of the commons).

(2) Is a much harder problem to solve and to a large extent it wouldn't go away even if we had a different internet.

And (2) is interesting because you don't necessarily need to compromise the target if you have control of the network infrastructure. For instance, China attacked GitHub by injecting JavaScript into people's navigation session (<http://www.netresec.com/?page=Blog&month=2015-03&post=China%27s-Man-on-the-Side-Attack-on-GitHub>). The Javascript code would then reach out to GitHub and DDoS the website.

Computer Science problem aside, (2) is problematic because it leads people to think that things like this: <http://www.skatingonstilts.com/skating-on-stilts/spiking-the-great-cannon.html> are a good idea.. These poor man's attempts at "sanctions" are not a solution, neither from a diplomatic/political POV nor from a technical one in my opinion.

Sent from my Iphone

On Sep 26, 2016, at 10:40, jeffrey E. <jeevacation@gmail.com> wrote:

<=lockquote type="cite">

http://fortune.com/2016/09/25/internet-infrastructure-attack/?xid=gn_editorspicks&google_editors_picks=true

--

= please note

The information contained in this communication is confidential, may be attorney-client privilege, may constitute inside information, and is intended only for the use of the addressee. It is the property of JEE. Unauthorized use, disclosure or copying of this communication or any part thereof is strictly prohibited and may be unlawful. If you have received this communication in error, please notify us immediately by return e-mail or by e-mail to jeevacation@gmail.com, and destroy this communication and all copies thereof, including all attachments. copyright -all rights reserved <<mailto:jeevacation@gmail.com>> =