SUNET

SHOWERTHOUGHTS: DDOSING AN IMPORTANT SOCIAL INSTITUTION (AND FIXING IT). PART1

So. I guess it is kind of timely that i decided to actually finalize this blogpost today when media has been blowing up lately that a DDOS that hit more or less all the news-sites in Sweden shut them down for a few hours. Initially this blogpost was designed as not based on a real story just a ”what-if” story but now that we have something fresh to talk about, lets refer to the real world.

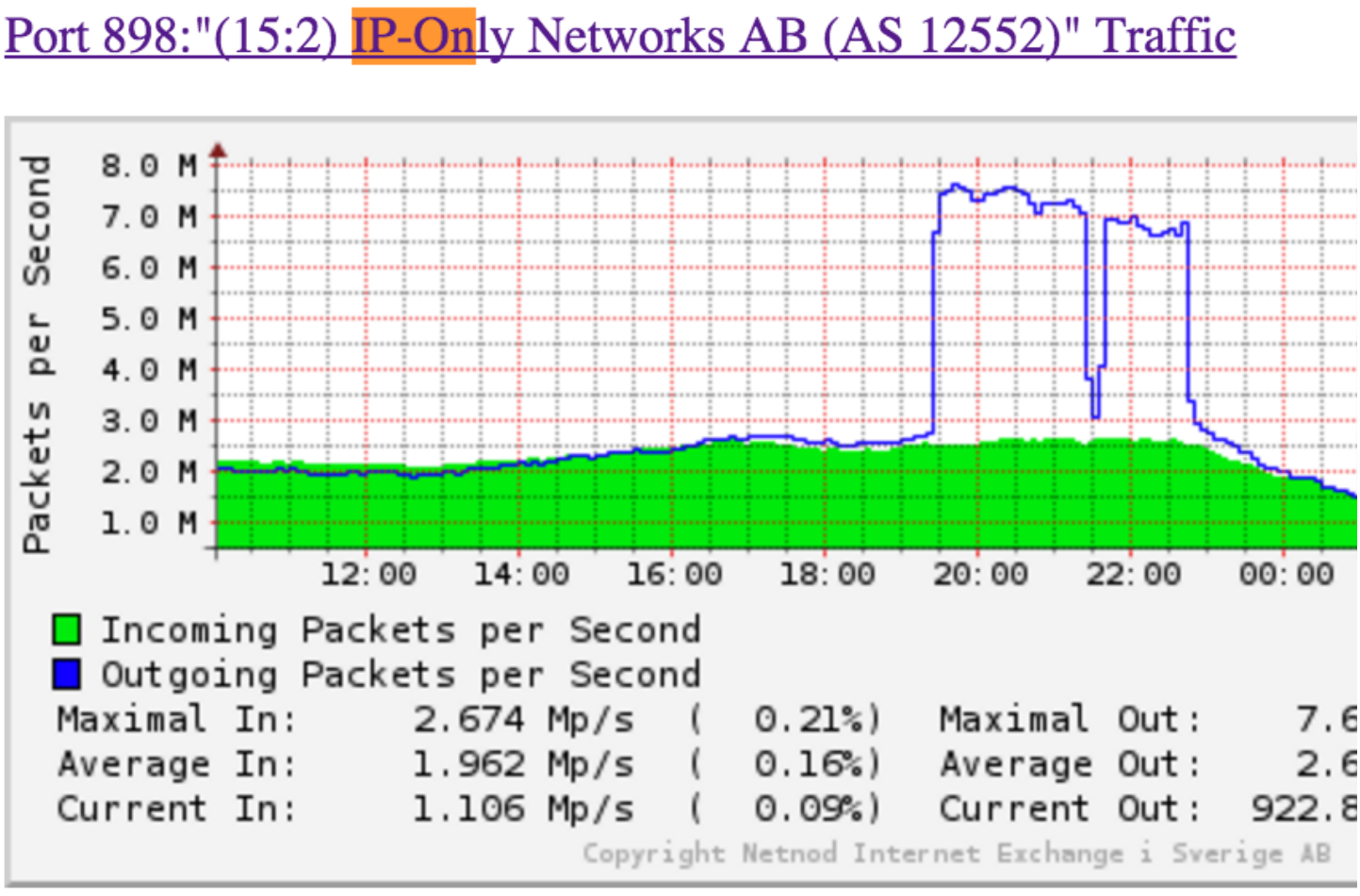
This is purely from a worried engineer’s point of view that has no affiliation to any of those affected.

This DDOS caused a storm (perhaps in a waterglass), a-lot of people including both the prime-minister and the minister of home-affairs making public statements about it and that Cyberwarfare is the next big thing etc blah blah. In the ISP-world dealing with DDOS is not really a new thing, we have seen this been happening for 15 years. The attack on the big Swedish newspapers was not anything spectacular or anything we have not seen before but shutting down all of the prime newspapers at the same time is an effective way of getting attention, especially from the media themselves.

So what actually happened? Well we don’t know all the details just right now but we can make a fair deal of assumptions taking in the things we actually know about.

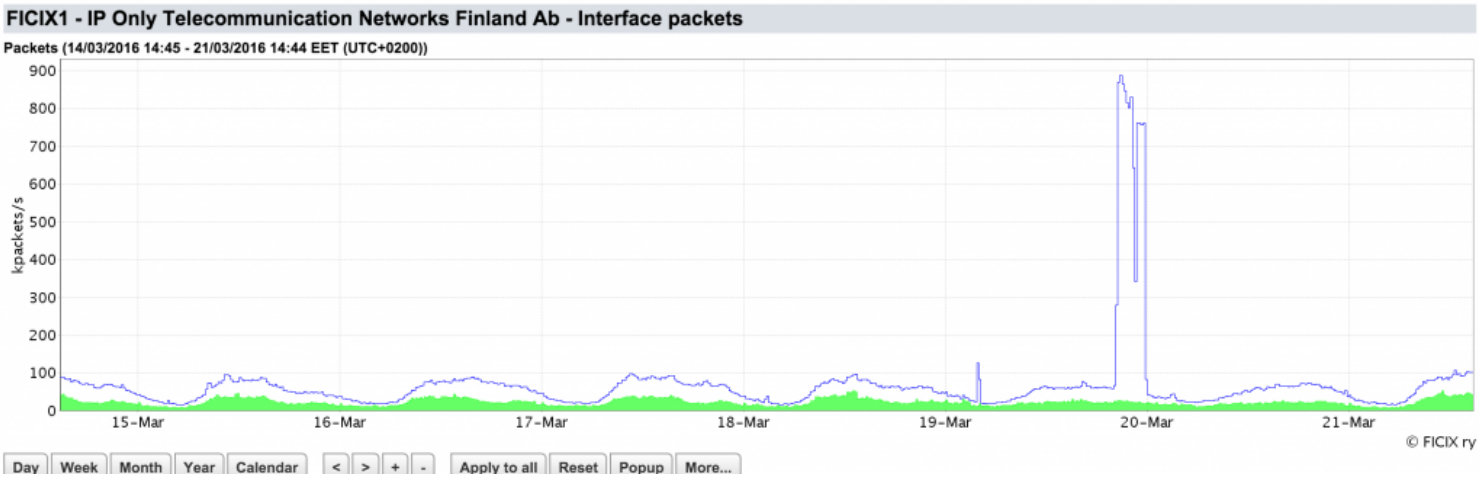
Fact 1: National news such as SVD, DN, DI. Aftonbladet. Expressen and local news such as VLT, HD, ÖP, NA and possibly more was more or less unreachable for a few hours during saturday evening due to someone or something ordered a DDOS-attack on all these media-outlets simultaneously

Fact 2: Press, media and social-media celebrities wasn’t late on blaming russia, or the ”east” for this. This is loosely based accusations based on the public network-statistics from Netnod.



Above we can see a suspicious pattern, IP-Only (which is a network-operator that host most media-sites in Sweden) has a huge influx of incoming packets from regular big russian operators. This indeed means that we can almost be very certain that these russian networks customers was indeed part of bringing down the sites, but they were not alone. What most people are missing is that this is just a very small part of the story. Netnod is not the only place where a network such as IP-Only exchanges traffic, IP-only exchanges traffic settlement-free with other networks on 14 other places, none of which has publicly available statistics to take part off except Netnod. We have no idea how much traffic that came in from Asia, India or South-America which is other more common places to generate DDOS from when in control of a botnet. This traffic is usually not interchanged over Netnod though since we do not have any brazilian networks exchanging traffic in Stockholm, we do have the russians though so that's why we can see how the russian traffic flows into IP-Only.

***EDIT 13:42 CET**. FICIX (The finnish Internet Exchange) also saw an influx of PPS to IP-Only at the same time, and they also have public statistics. And this was also primarly from a russian operator*



From an outside perspective we have no idea how much traffic IP-only received through their regular IP-transit either. This could be ten times as much, or ten times as little, we do not know and probably never will seeing as this is is not public information and will probably never be unfortunately. But judging of the size of the company, comparing routing-tables and using BGP looking-glasses we can make the assumption that IP-Only relies quite heavily on taking in non-nordic traffic through their transit-provider.

We do not know either where this traffic caused congestion. It could have been somewhere in IP-Onlys edge-network, in their core-network, or in their customer-facing part of the network. Obviously the port on Netnod was not congested in terms of bandwidth atleast, but other then that, its just speculations.

Alright, twittertime.

This makes a tweetfest like this from a competing company's CEO (Bahnhof) to look very uneducated/sensationalist and technically incorrect (sorry english readers) from a engineer's point of view. While Jon is famous for not keeping back on social-media especially regarding Integrity and i usually applaud him for that i don't agree that making uneducated claims like this is the way forward.

Looking at our own network (this time i'm speaking with the NORDUnet hat on) which is under constant DDOS of small and big attacks we do see that botnets from the russian operators is usual suspects when it comes to DDOS but far from alone. This is the top source-asns that our netflow-analyzer (deepfield) counts as DDOS-traffic using data from the last 6 months.

1. Beeline / Vimpelcom AS8402, Russia
2. Comcast AS7922, USA
3. Choopa AS20473, USA
4. China Telecom, AS23724, China
5. China Telecom (another AS), AS4134, China
6. Nforce AS43350, Netherlands
7. Golden Telecom / Sovintel AS3216, Russia
8. China Unicom AS4837, China
9. Cox AS22773, USA
10. DigitalOcean AS202018, Everywhere
11. HiNet AS3462, Taiwan
12. Ziggo AS9143, Netherlands
13. China Telecom (another as again) AS58543, China
14. PCCW AS4760, South-East Asia
15. TurkTelecom AS9121, Turkey

So. This is DDOS over a extensive period of time and a-lot of these networks is accumulating positions on our DDOS shitlist just because they are very big networks and its hard to keep track of their million of million of subscribers. Im not excusing them in anyway way but if your network grows at the pace of one Sweden, per year, some things might be on the backburner, such as security. Eventually these subscribers will put unpatched Windows XP boxes on the internet and become part of a botnet within a few seconds and partake as on-demand-ddos drones. While our split of ddos-networks might not look similar to anyone else, we could assume at least that some of the aforementioned networks took part. The russian networks in our list is definitely on the list that attacked the media.

Fact3: ”This is a expensive and well thought out operation that could be a test for something bigger, just when burglars trips the alarm on the bank to see how long it takes for the cop to get there”.

Possibly, it could also be a bored teenager with a few hundreds Euros to spare. DDOS is not expensive, at all. You can hire botnets by the hour on the darker side of the Internets and last time i checked (when we got hit by a NTP amplficated 70Gbps DDOS that caused disturbance) the hourly price on that type of attack was about 1 Bitcoin/hour, which today is somehwere around 300Euro/hour. Even if this attack used a slightly different approach (tcp-syn, fragments and smallest possible packets etc) lets assume the pricing is somewhat similar . This is within reach from everything to oppresive regimes, to criminal syndicates and bored teenagers from Åmål. Speculating does us no good here and just acts as scareware.

Fact4: ”Mitigating attacks like this is almost impossible and requires the operator to invest alot of money into ddos-mitigating devices”

Yes, and no.

Yes, magical DDOS-mitigation-devices is extremely expensive, that is correct. A company such as Arbor make a decent living on DDOS-mitigation devices. And in recent times companys such as Prolexic and Staminus has popped up aswell as ”cloud-ddos-mitigation” companys and seeing as Staminus just recently got completly defaced and billing-informationed leaked out, we know that they are making a really good chunk of money aswell.

No, mitigating these attacks with smart methods is not expensive. Complicated perhaps, but not expensive. Most methods is usually free! Which i like, but i’ll talk more about that in part2 since i want this text out before the whole things blow over and no one cares about this until next time it happens.

Skriven av

FREDRIK “HUGGE” KORSBÄCK

Network architect and chaosmonkey for AS1653 and AS2603. Fluent in BGP hugge@nordu.net