

HPIMP: Measuring Booter Services

RIPE MEETING

77

Amsterdam, Netherlands
15 - 19 Oct 2018



Where networks meet

*Daniel Kopp
DE-CIX Products & Research*

www.de-cix.net

DDoS & Botter Services

- We see DDoS attacks on a daily basis at IXPs
- What's their origin?
- How bad is it?
- Understand the capabilities and the threat
- We build a dedicated system to record DDoS by attacking ourselves

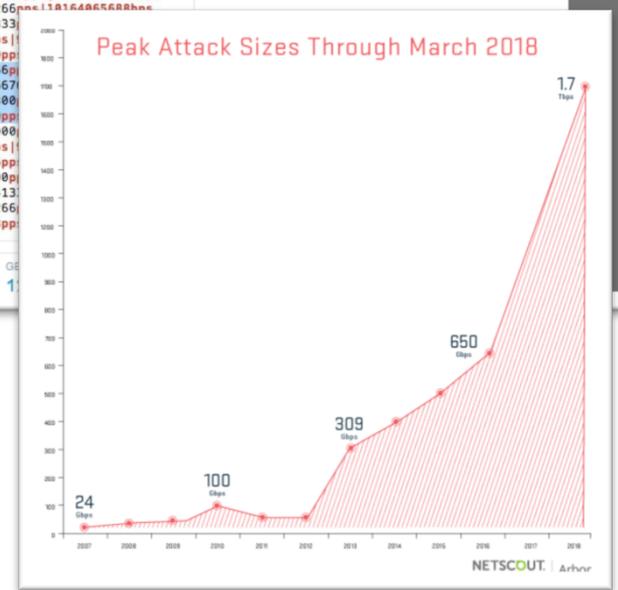


Octave Klaba / Oles
@olesovhcom

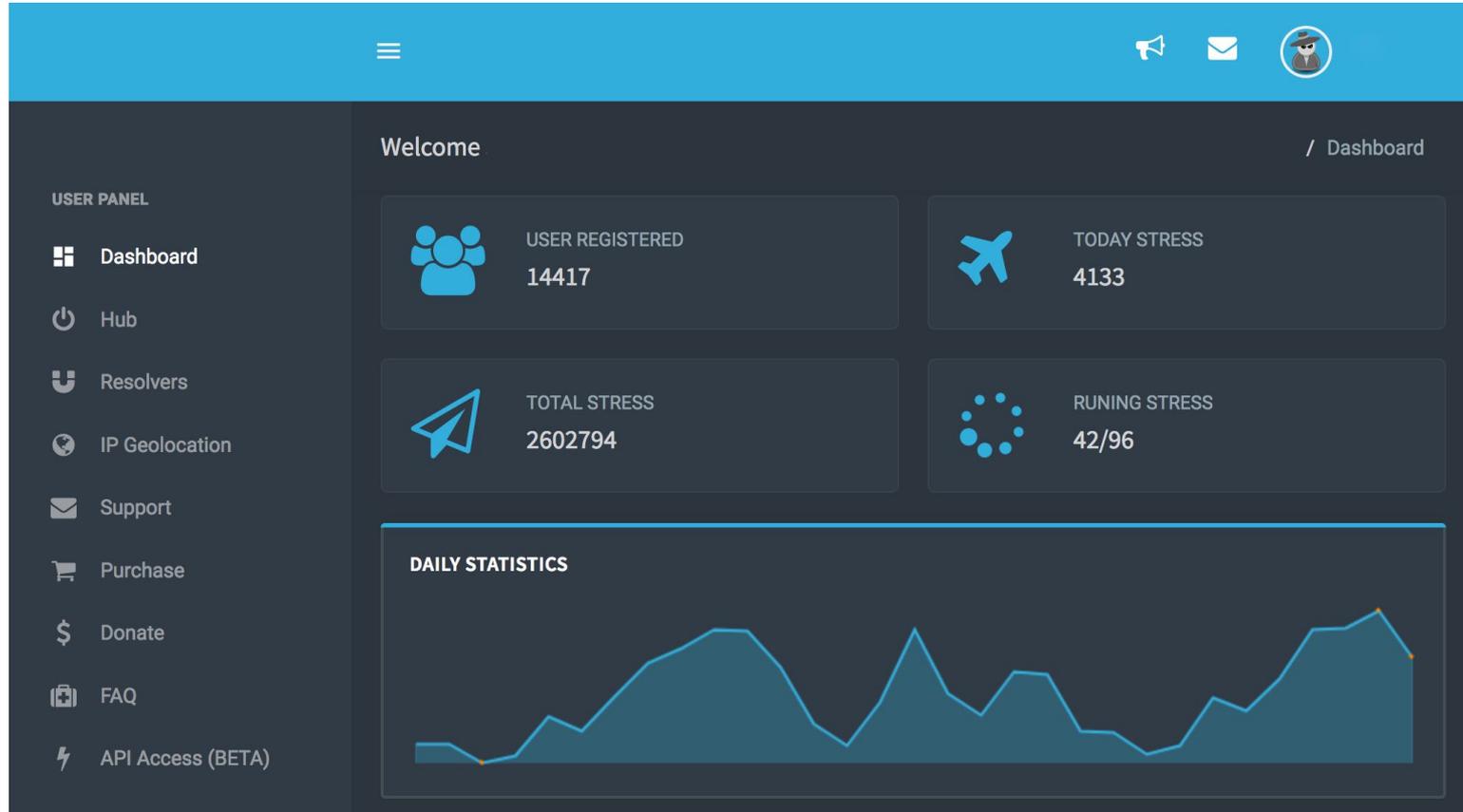
@Dominik28111 we got 2 huge multi DDoS: 1156Gbps then 901Gbps

141822 | 961266 | 11518142pps | 900 | 3450300pps | 040 | 22434666pps | 007039 | 937667 | 41900 | 3450300 | 92 | 16026379pps | 7045 | 25634000 | 11529383pps | 959 | 7555266pps | 044 | 14566000pps | 007045 | 722413 | 41959 | 7555266pps | 51 | 11529383pps

RETWEETS 138



Example - Dashboard



Example - Serviceplans

The dashboard features a dark sidebar on the left with navigation items: Dashboard, Boot, Tickets, Help, Purchase with BTC, and Purchase with ETH. The main content area has a 'Welcome' message, a warning banner, and a grid of service plans.

Welcome
Your **reliable** stresser.

Warning
You cannot purchase a new membership right now. Note: You already have a membership. You can buy when your current membership expire.

Available Packages - Instant Delivery

Silver	Gold	Platinum
\$14/month	\$19/month	\$29/month
600 seconds boot time All methods 1 concurrent 30 days Instant delivery	1200 seconds boot time All methods 1 concurrent 30 days Instant delivery	1800 seconds boot time All methods 1 concurrent 30 days Instant delivery
PURCHASE	PURCHASE	PURCHASE

VIP Silver	VIP Gold	VIP Platinum
\$79/month	\$89/month	\$119/month
4800 seconds boot time All methods 1 concurrent 30 days Instant delivery	7200 seconds boot time All methods 1 concurrent 30 days Instant delivery	10800 seconds boot time All methods 1 concurrent 30 days Instant delivery
PURCHASE	PURCHASE	PURCHASE

Order Confirmation

Description: Add Service access

Seconds: 1200 (20 Minutes)
Concurrents: 1 (Simultaneous Running Floods)
Targets per Day: 40 (Resets every day at midnight, our server time)
Length: 1 Months
VIP Access: ❌
API Access: ❌
Price: \$22.80 USD
Crypto Price: \$19.38 USD

PROCEED TO CHECKOUT

Order Confirmation

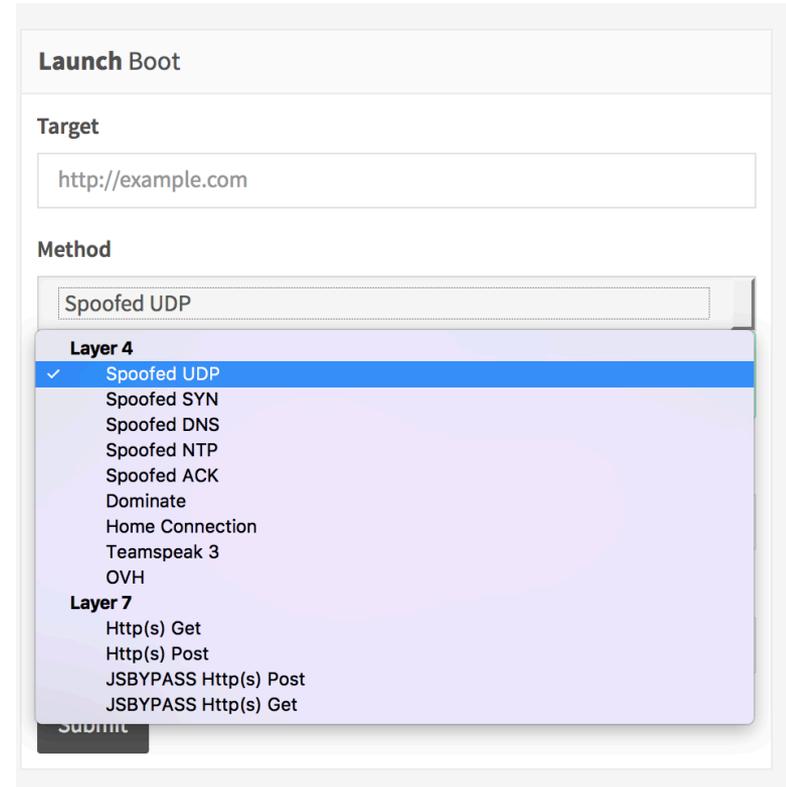
Description: Add Service access

Seconds: 1200 (20 Minutes)
Concurrents: 1 (Simultaneous Running Floods)
Targets per Day: 40 (Resets every day at midnight, our server time)
Length: 1 Months
VIP Access: ✔️
API Access: ❌
Price: Cannot exceed \$75.00 USD, crypto checkout available only!
Crypto Price: \$178.84 USD

PROCEED TO CHECKOUT

Example – DDoS Order

- Flat rate for DDoS attacks
 - x attacks a day
 - x concurrent
 - Usually 30 days
- 10 - 20 different types
 - Application → high pps
 - Amplification → high bandwidth
- Claim to offer 5 - 100 Gbit/s



Launch Boot

Target

http://example.com

Method

Spoofed UDP

Layer 4

- ✓ Spoofed UDP
- Spoofed SYN
- Spoofed DNS
- Spoofed NTP
- Spoofed ACK
- Dominate
- Home Connection
- Teamspeak 3
- OVH

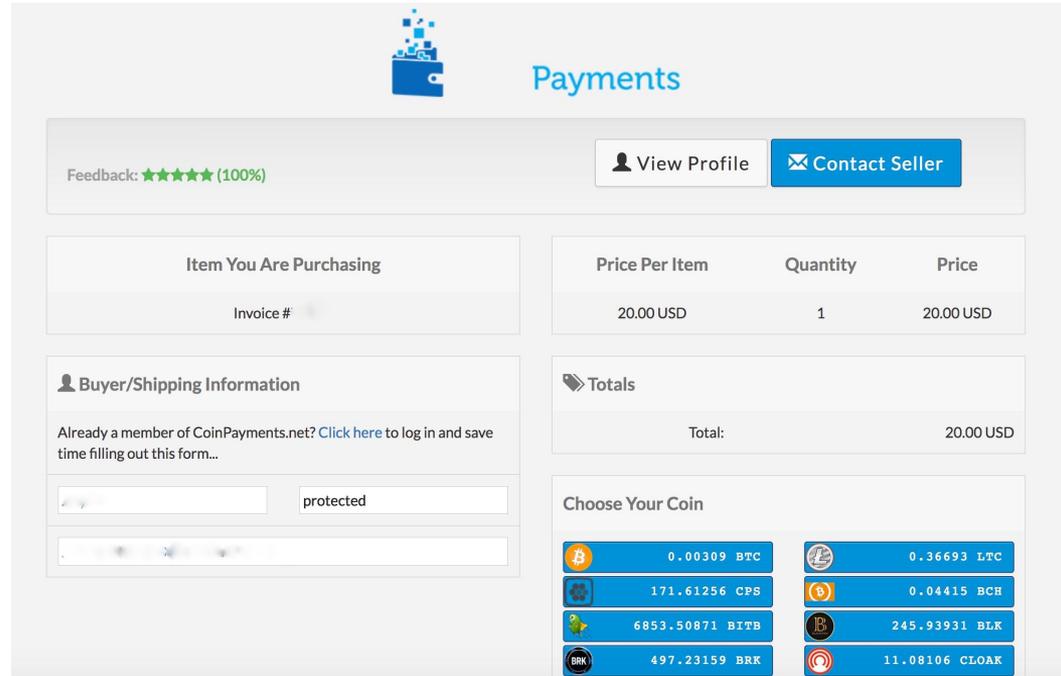
Layer 7

- Http(s) Get
- Http(s) Post
- JSBPASS Http(s) Post
- JSBPASS Http(s) Get

Submit

Payment

- Fake services exist
- Payment with crypto currency
- Payment and activation takes time
- Prices vary \$20 - \$200



The screenshot shows a payment interface for a seller. At the top, there is a logo and the word "Payments". Below this, there is a feedback section showing a 5-star rating (100%) and two buttons: "View Profile" and "Contact Seller".

The main content area is divided into several sections:

- Item You Are Purchasing:** A table with columns "Price Per Item", "Quantity", and "Price". The price per item is 20.00 USD, the quantity is 1, and the total price is 20.00 USD.
- Buyer/Shipping Information:** A section with a heading "Buyer/Shipping Information" and a message: "Already a member of CoinPayments.net? [Click here](#) to log in and save time filling out this form...". Below this are two input fields, one of which contains the text "protected".
- Totals:** A section with a heading "Totals" and a table showing "Total: 20.00 USD".
- Choose Your Coin:** A section with a heading "Choose Your Coin" and a grid of buttons for different cryptocurrencies. Each button shows the coin's icon, the amount, and the coin's symbol.

Price Per Item	Quantity	Price
20.00 USD	1	20.00 USD

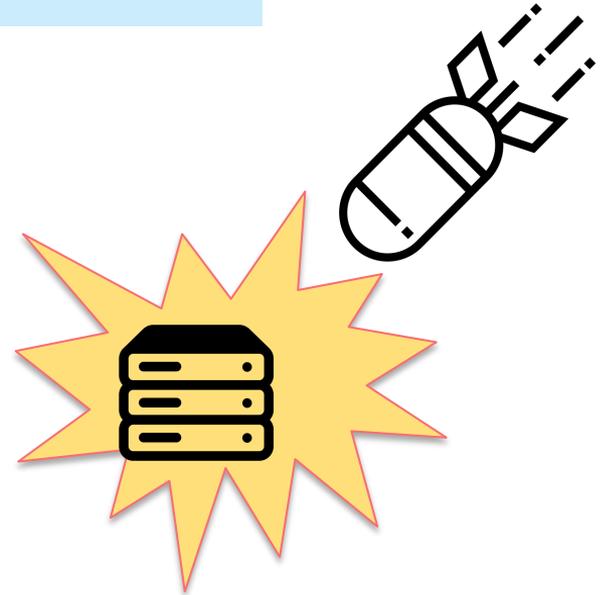
Totals	
Total:	20.00 USD

Choose Your Coin	
 0.00309 BTC	 0.36693 LTC
 171.61256 CPS	 0.04415 BCH
 6853.50871 BITB	 245.93931 BLK
 497.23159 BRK	 11.08106 CLOAK

Measurement System Motivation

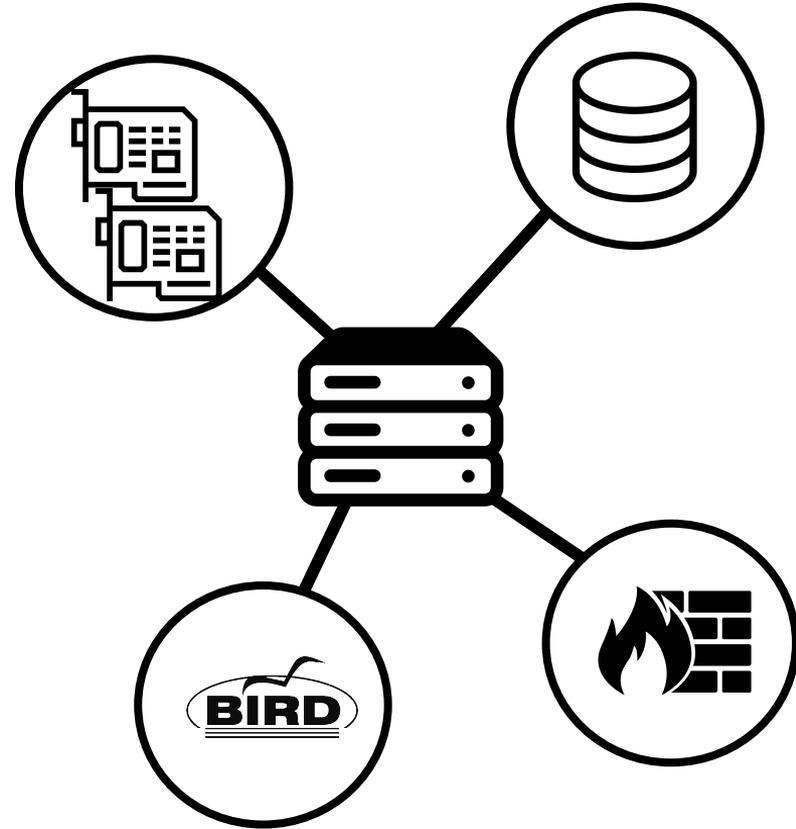
We built a server and network setup to attack ourselves and record the attack traffic

- **Requirements**
 - **Minimal impact during DDoS**
 - **Record 10 Gbit/sec to disc**
 - **Record at least continuous 30min**
 - **Global reachability**
 - **Direct connection to many ASNs**
 - **Keep costs low**



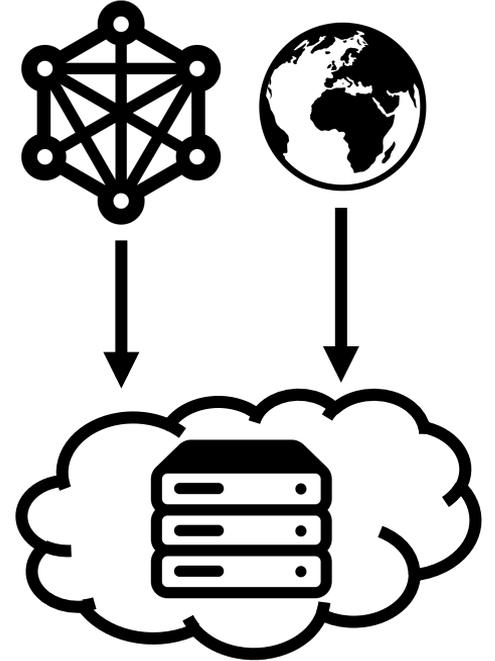
Measurement System and Setup

- **Hardware**
 - Dedicated second NIC as mirror
 - Fast write speed: SAS RAID-0
 - Dedicated Raid Controller
 - Single core performance
- **System Setup**
 - Linux as a BGP Router and Network
 - Bird & Docker
 - ARP! → ARP tables and IP tables

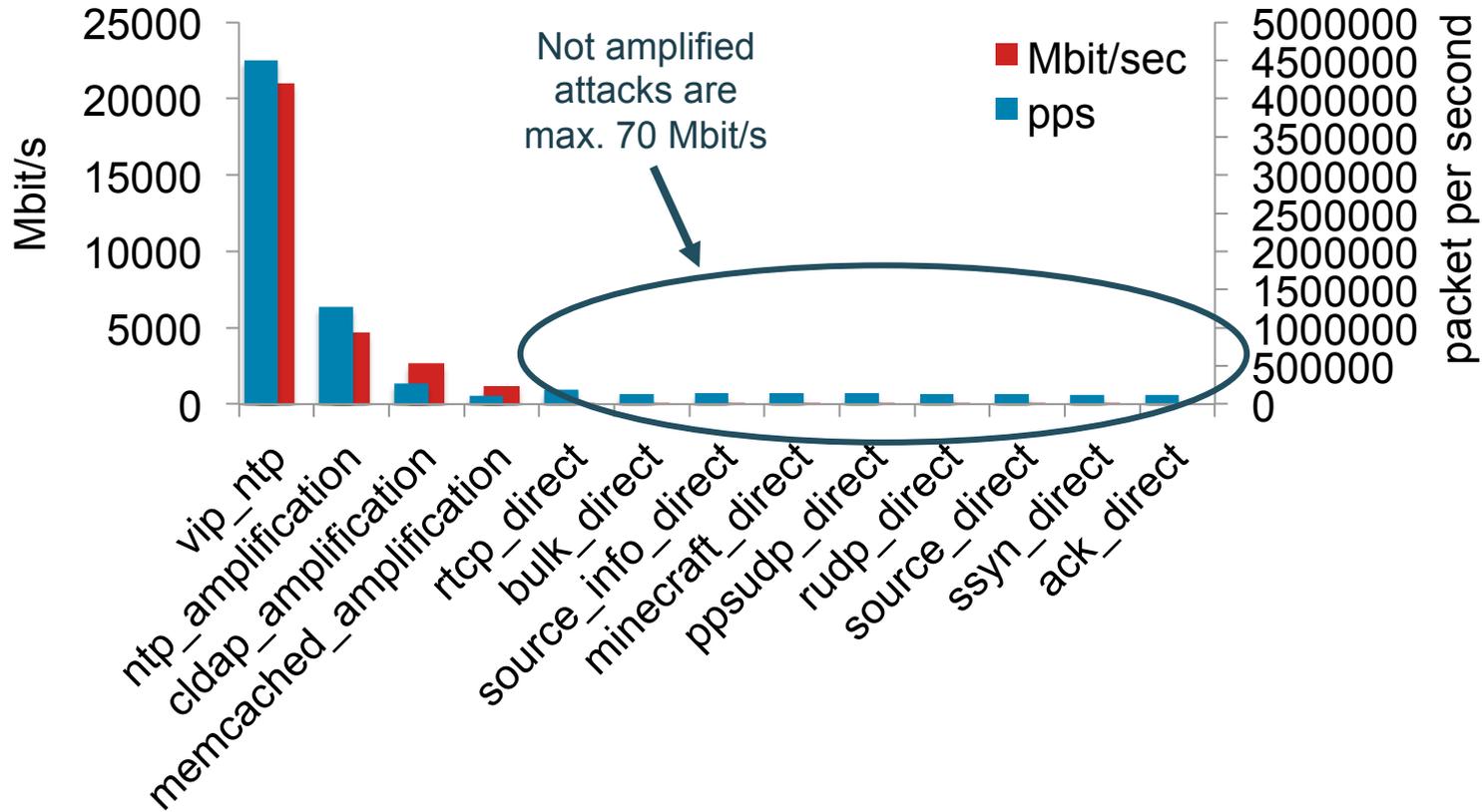


Measurement System and Setup

- **Internet Connectivity**
 - 10G Peering
 - 10G Transit
 - Own ASN and IPv4 Space
- **Measurement Limitations**
 - Tcpcap → up to 10 Gbits/sec
 - sFlow → up to 10 Gbits/sec
 - IPFIX → over 100 GBit/secs

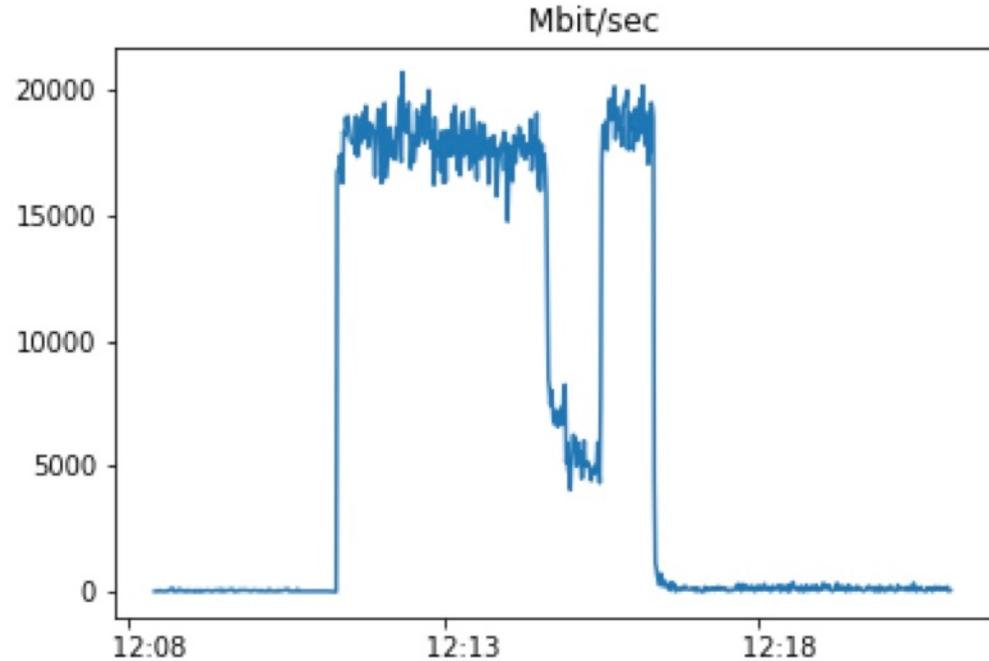


DDoS Attacks - Overview



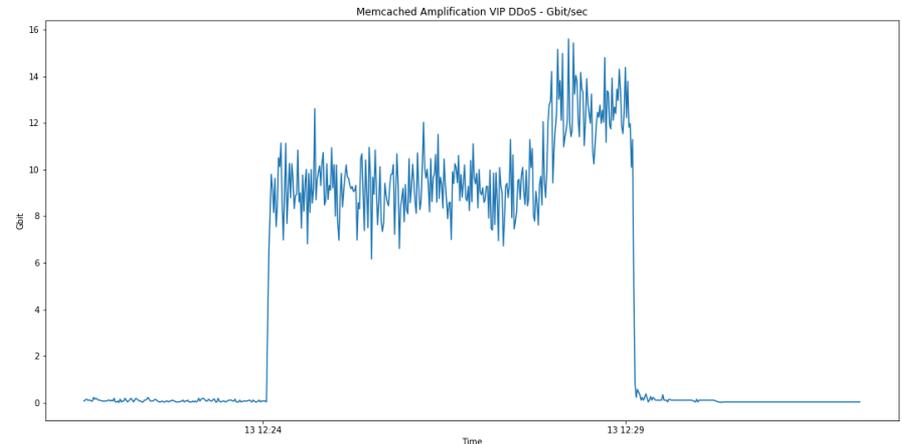
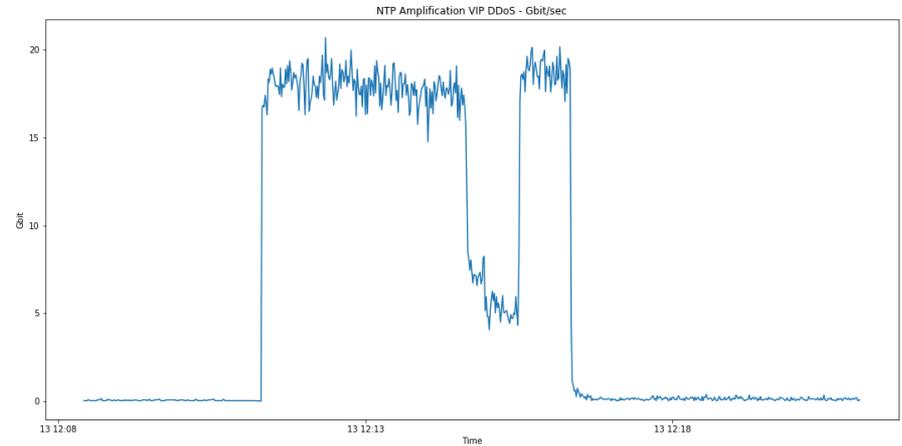
DDoS - NTP Reflection

- **20 Gbit/s**
- **4 million pps**
- **930 source IPs**
- **350 source ASNs**
- **Top 3 ASes 23% of traffic**
 - **China, Taiwan, Hungary**
- **80% of traffic over transit**



DDoS – NTP vs. Memcached Reflection

- **20 Gbit/s NTP**
 - **930 reflectors**
 - **350 ASNs**
- **15 Gbit/s MEMCACHED**
 - **300 reflectors**
 - **150 ASNs**
- **Location of NTP reflectors mostly Asia**
- **Location of Memcached reflectors mostly Europe**



Summary and Future Work

- **Summary**
 - **Many different attack types**
 - **Prices from \$20 - \$200**
 - **Flat rate for DDoS attacks**
 - **Recorded 5 – 20 GBit/s**
 - **Only amplified attacks provided high bandwidth**

- **Future Work**
 - **Build mitigation strategies**
 - **Understand anatomy of attacks**
 - **Pinpoint problems e.g. open resolvers or botnets**

A person is holding a globe of the Earth in front of a wall covered in newspaper clippings. The globe is the central focus, showing continents and oceans. The text 'Q&A - Discussion - Feedback' is overlaid in white, bold, sans-serif font across the middle of the image.

Q&A - Discussion - Feedback



Where networks meet

www.de-cix.net