

HPIMP: Measuring Booter Services

RIPE MEETING

77

Amsterdam, Netherlands
15 - 19 Oct 2018



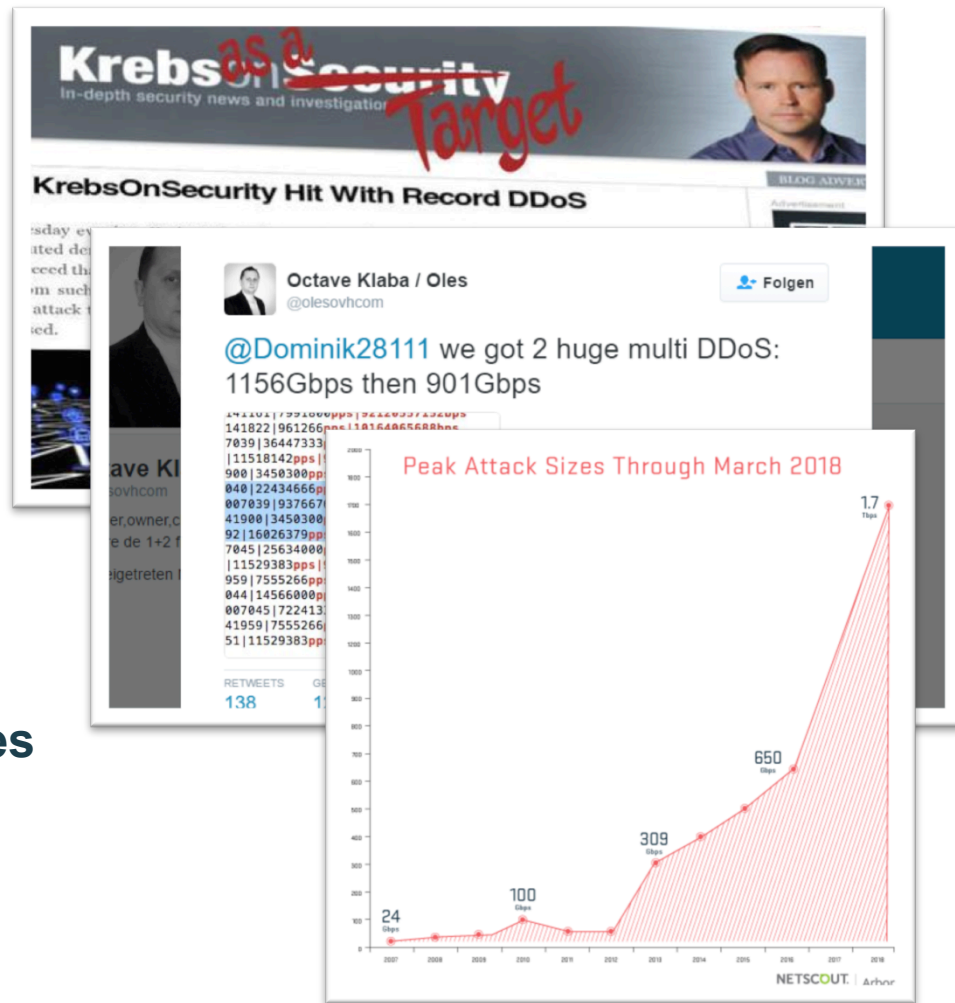
Where networks meet

*Daniel Kopp
DE-CIX Products & Research*

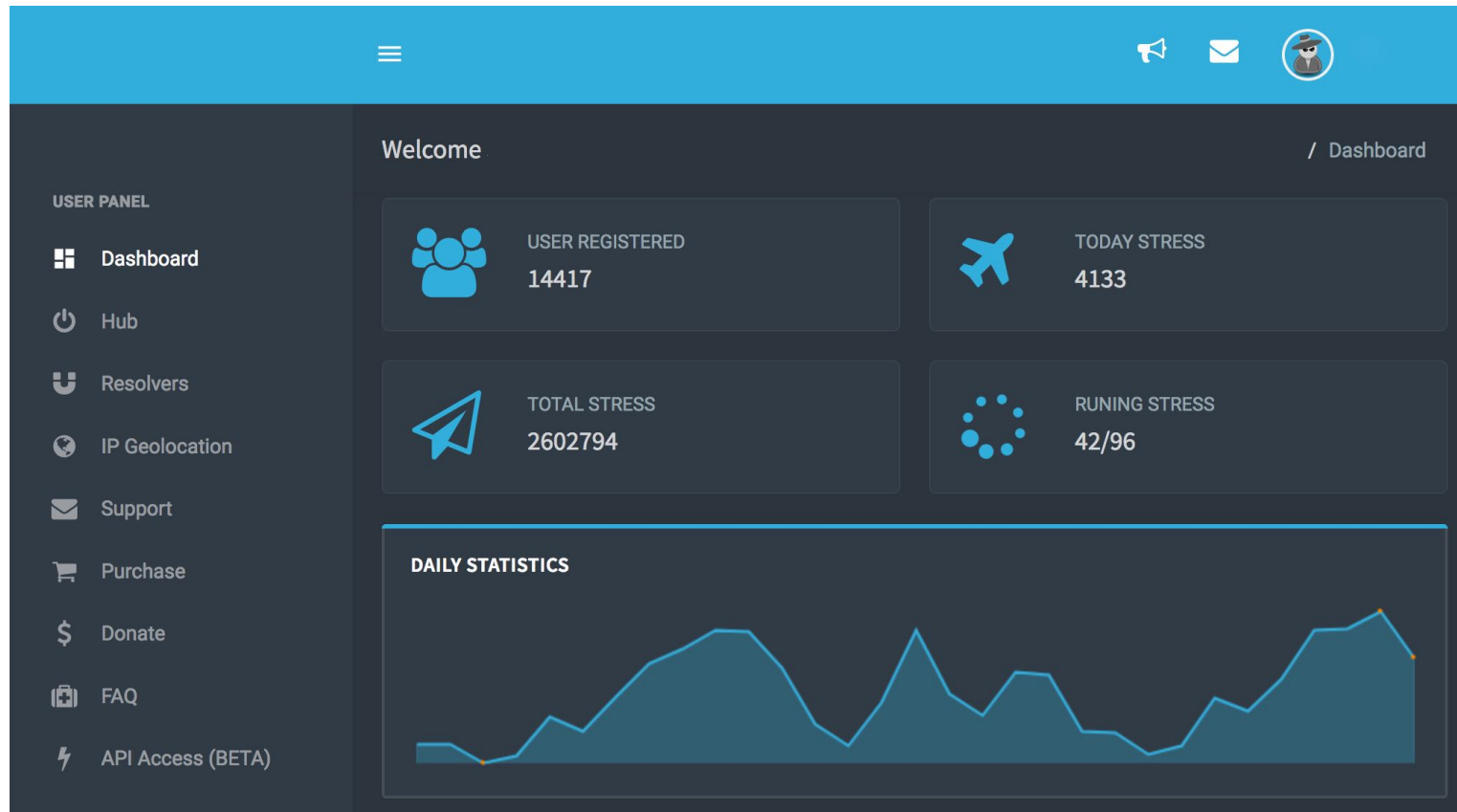
www.de-cix.net

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



Example - Dashboard



Example - Serviceplans



Dashboard

Boot

Tickets

Help

Purchase with BTC

Purchase with ETH

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

\$14/month

600 seconds boot time

All methods

1 concurrent

30 days

Instant delivery

PURCHASE

Gold

\$19/month

1200 seconds boot time

All methods

1 concurrent

30 days

Instant delivery

PURCHASE

Platinum

\$29/month

1800 seconds boot time

All methods

1 concurrent

30 days

Instant delivery

PURCHASE

VIP Silver

\$79/month

4800 seconds boot time

All methods

1 concurrent

30 days

Instant delivery

PURCHASE

VIP Gold

\$89/month

7200 seconds boot time

All methods

1 concurrent

30 days

Instant delivery

PURCHASE

VIP Platinum

\$119/month

10800 seconds boot time

All methods

1 concurrent

30 days

Instant delivery

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: ✗

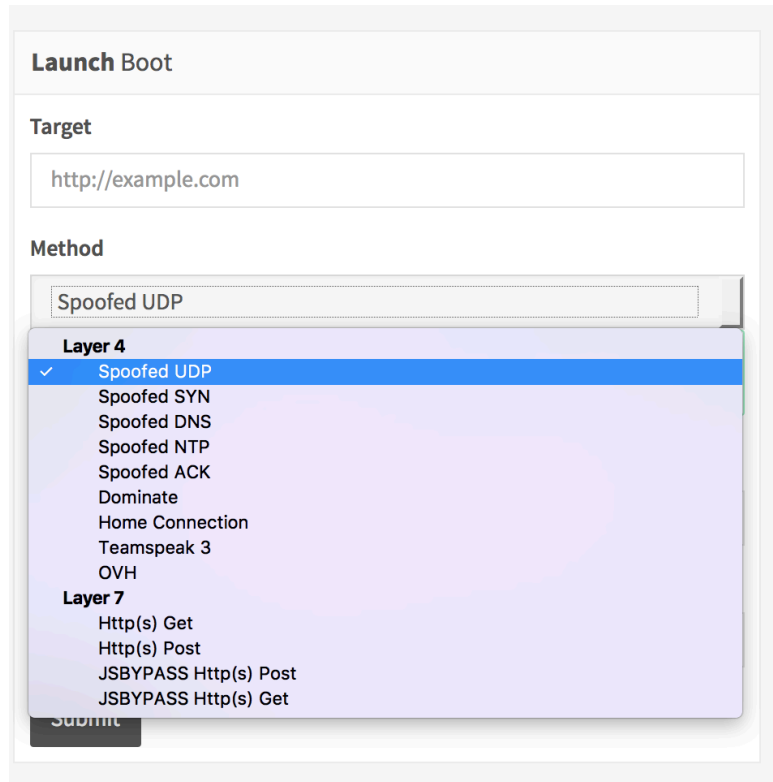
Price: Cannot exceed \$75.00 USD, crypto checkout available only!

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



The screenshot shows a web interface for launching a DDoS attack. At the top is a header 'Launch Boot'. Below it is a 'Target' section with a text input field containing 'http://example.com'. Underneath is a 'Method' section with a dropdown menu currently showing 'Spoofed UDP'. A modal window is open, displaying a list of attack methods categorized by layer. 'Layer 4' is expanded, showing options like 'Spoofed UDP' (which is selected with a checkmark), 'Spoofed SYN', 'Spoofed DNS', 'Spoofed NTP', 'Spoofed ACK', 'Dominate', 'Home Connection', 'Teamspeak 3', and 'OVH'. Below this, 'Layer 7' is also listed with options like 'Http(s) Get', 'Http(s) Post', 'JSBYPASS Http(s) Post', and 'JSBYPASS Http(s) Get'. A 'Submit' button is visible at the bottom of the modal.

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

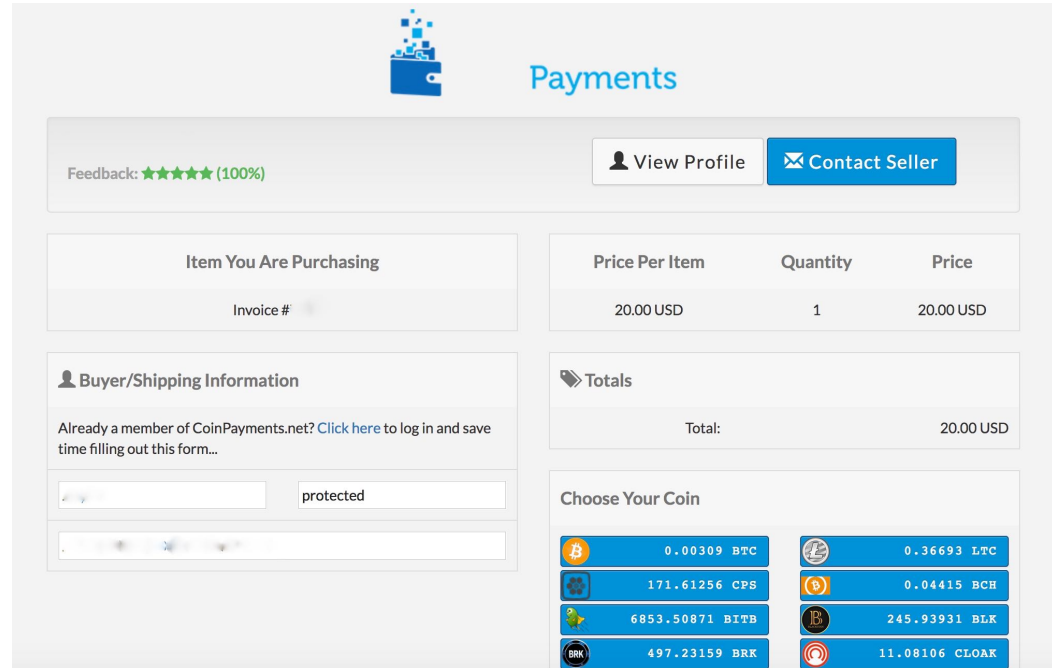
Layer 7

- Http(s) Get
- Http(s) Post
- JSBYPASS Http(s) Post
- JSBYPASS Http(s) Get

Submit

Payment

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



The screenshot shows the CoinPayments.net checkout page. At the top, there's a blue icon of a wallet with coins and the word "Payments" in blue. Below this, a feedback bar shows "Feedback: ★★★★★ (100%)". To the right are buttons for "View Profile" and "Contact Seller". The main content area is divided into several sections. On the left, under "Item You Are Purchasing", there's a placeholder for an invoice number. Below that is the "Buyer/Shipping Information" section, which includes a login prompt and a form with a "protected" label. On the right, there's a table showing the price per item (20.00 USD), quantity (1), and total price (20.00 USD). Below the table is a "Totals" section showing the total amount. At the bottom right, there's a "Choose Your Coin" section with a grid of buttons for different cryptocurrencies and their corresponding amounts.

Price Per Item	Quantity	Price
20.00 USD	1	20.00 USD

Totals

Total:	20.00 USD
--------	-----------

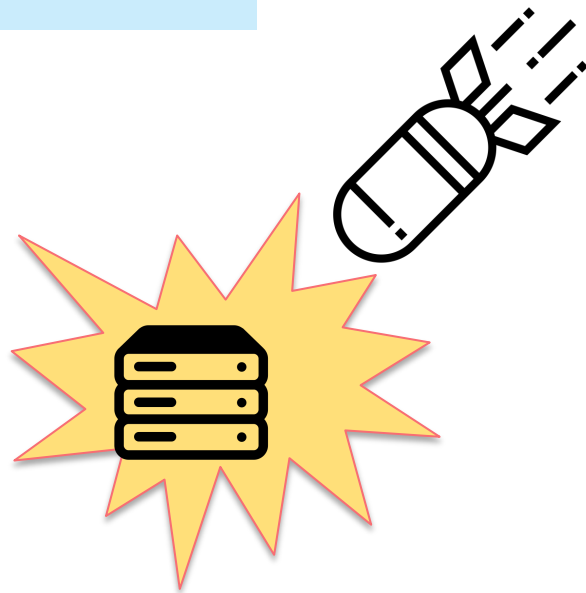
Choose Your Coin

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

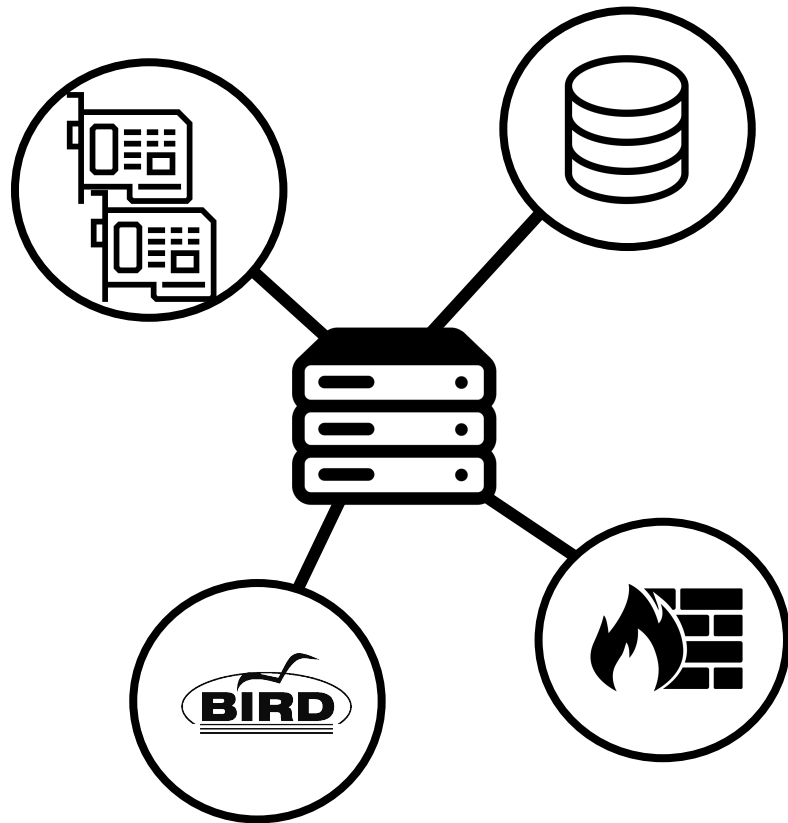
We built a server and network setup to attack ourselves and record the attack traffic

- **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**



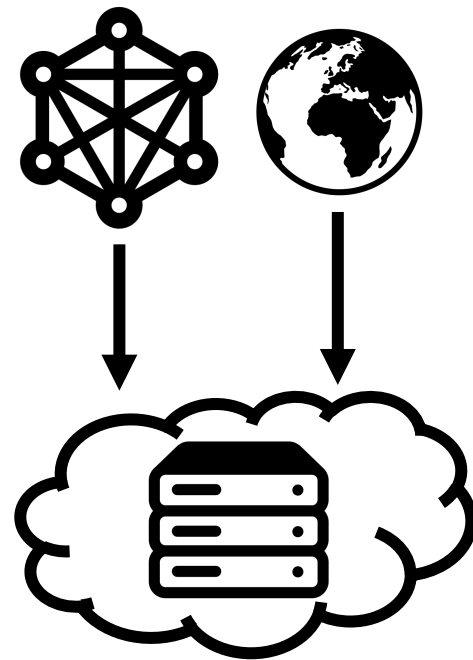
Measurement System and Setup

- **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

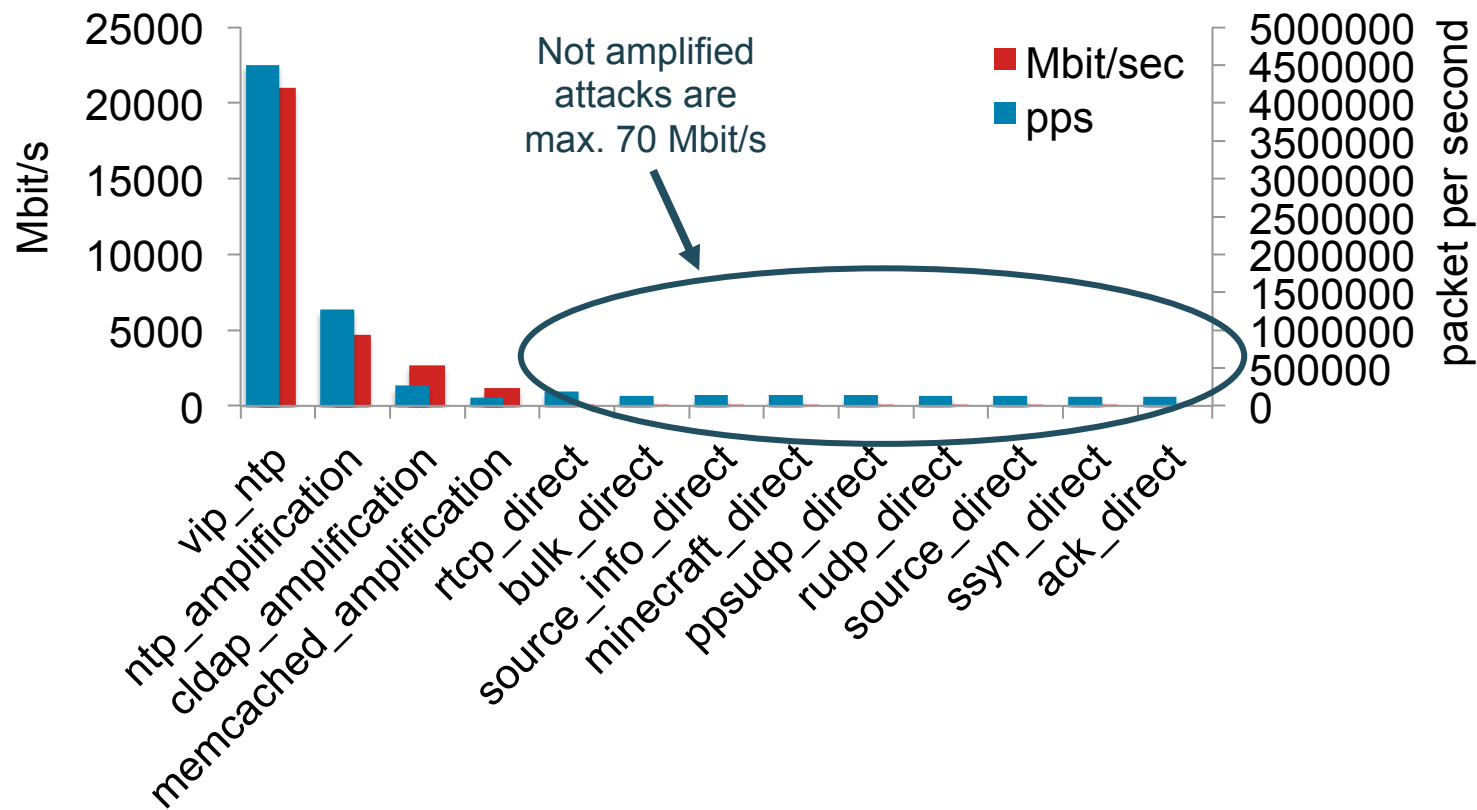


Measurement System and Setup

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

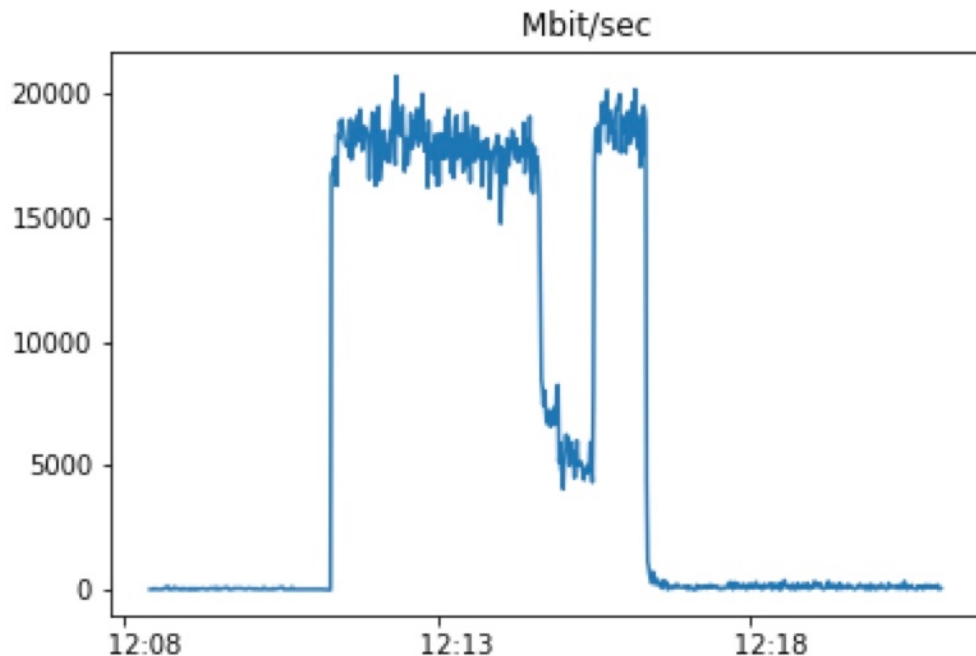


DDoS Attacks - Overview



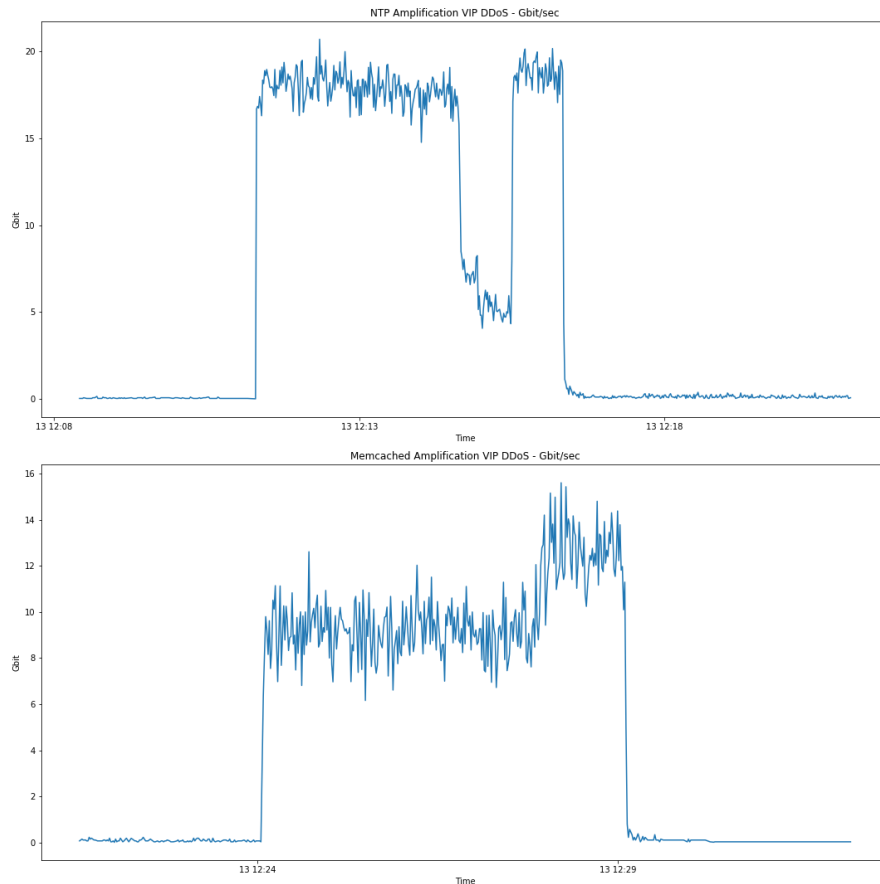
DDoS - NTP Reflection

- **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 vintage-style globe with both hands. The globe shows the continents of Africa, Europe, and Asia. The background is a wall covered in a collage of newspaper clippings and small photographs. The text "Q&A - Discussion - Feedback" is overlaid in the center in a white, bold, sans-serif font.

Q&A - Discussion - Feedback