HPIMP: Measuring Booter Services

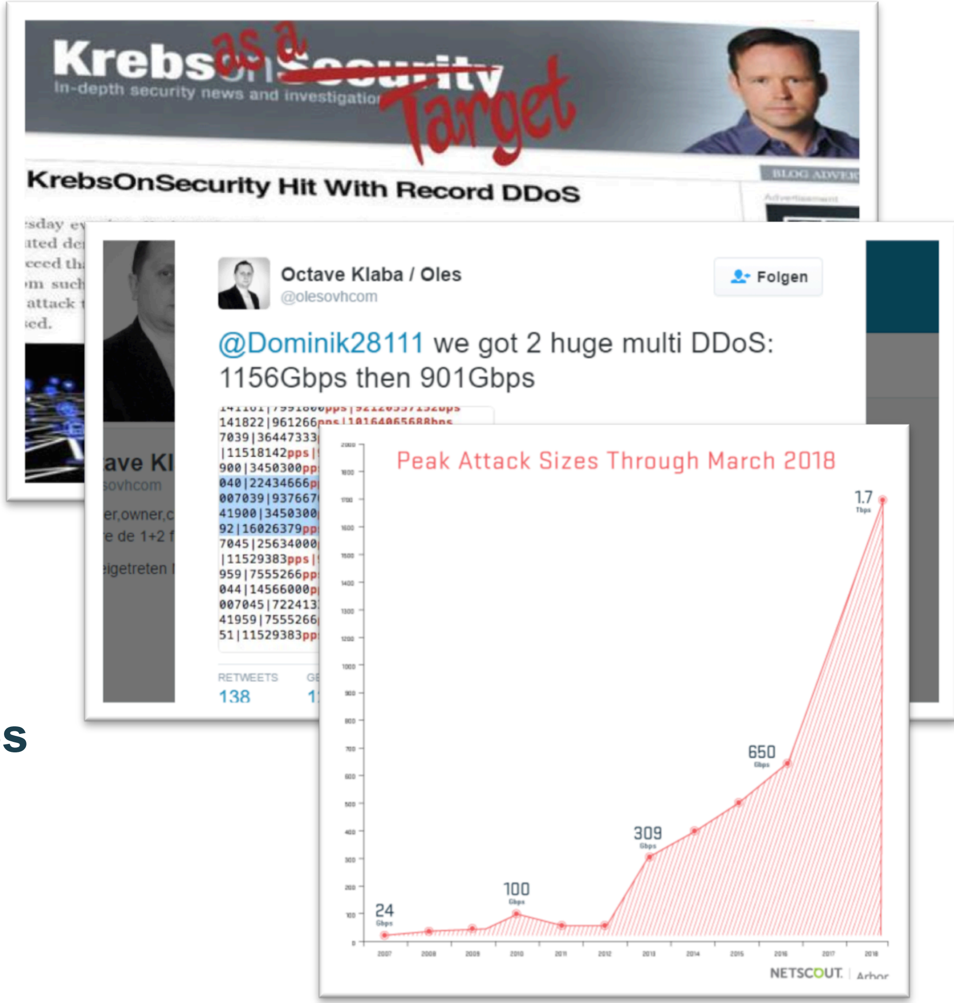
RIPE MEETING
77
Amsterdam, Netherlands
15 – 19 Oct 2018

DE CIX

Daniel Kopp
DE-CIX Products & Research

DDoS & Booter 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

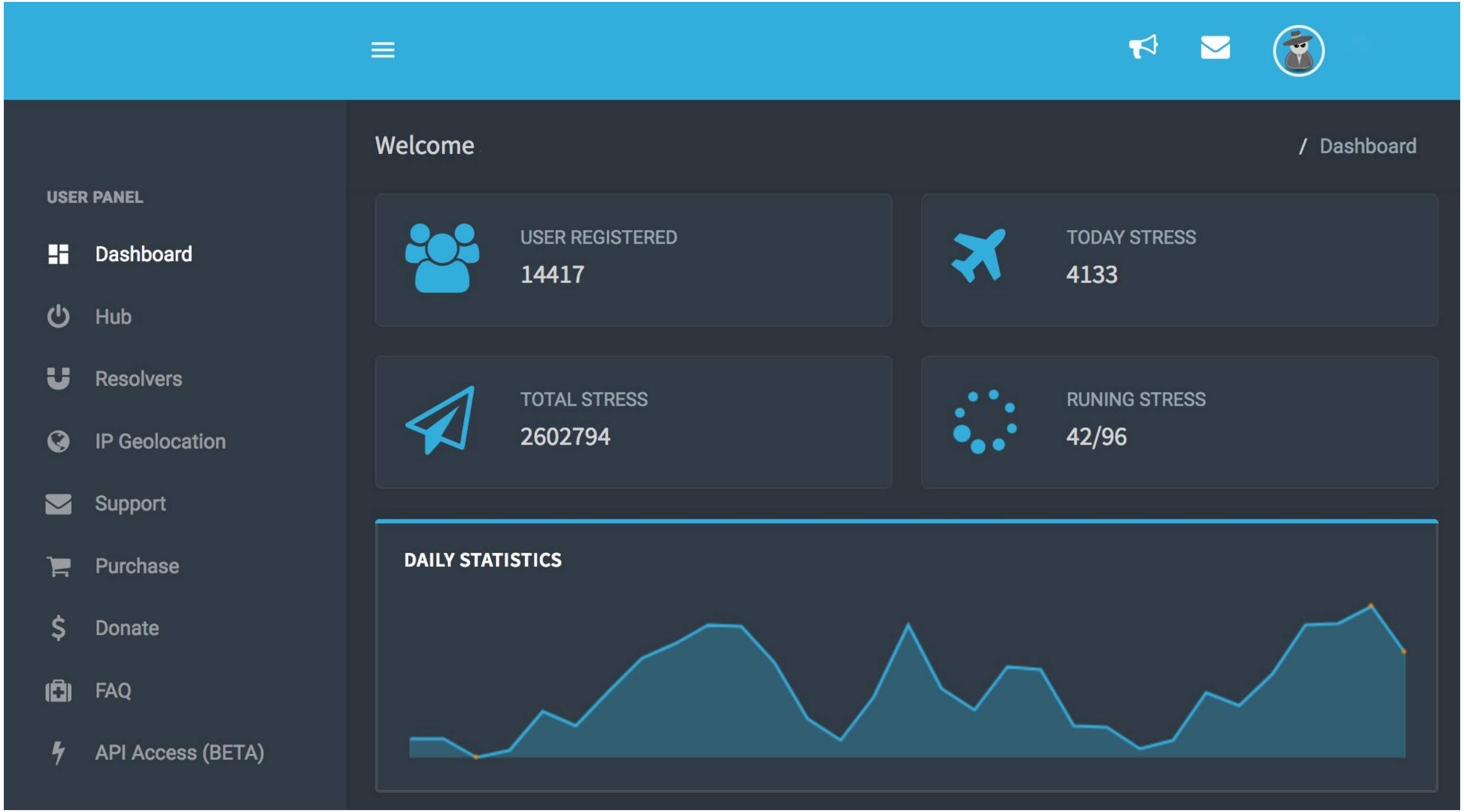


KrebsOnSecurity Hit With Record DDoS

Octave Klaba / Oles
@olesovhcom

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

Example - Dashboard



Welcome

/ Dashboard

USER PANEL

- Dashboard
- Hub
- Resolvers
- IP Geolocation
- Support
- Purchase
- Donate
- FAQ
- API Access (BETA)

USER REGISTERED

14417

TODAY STRESS

4133

TOTAL STRESS

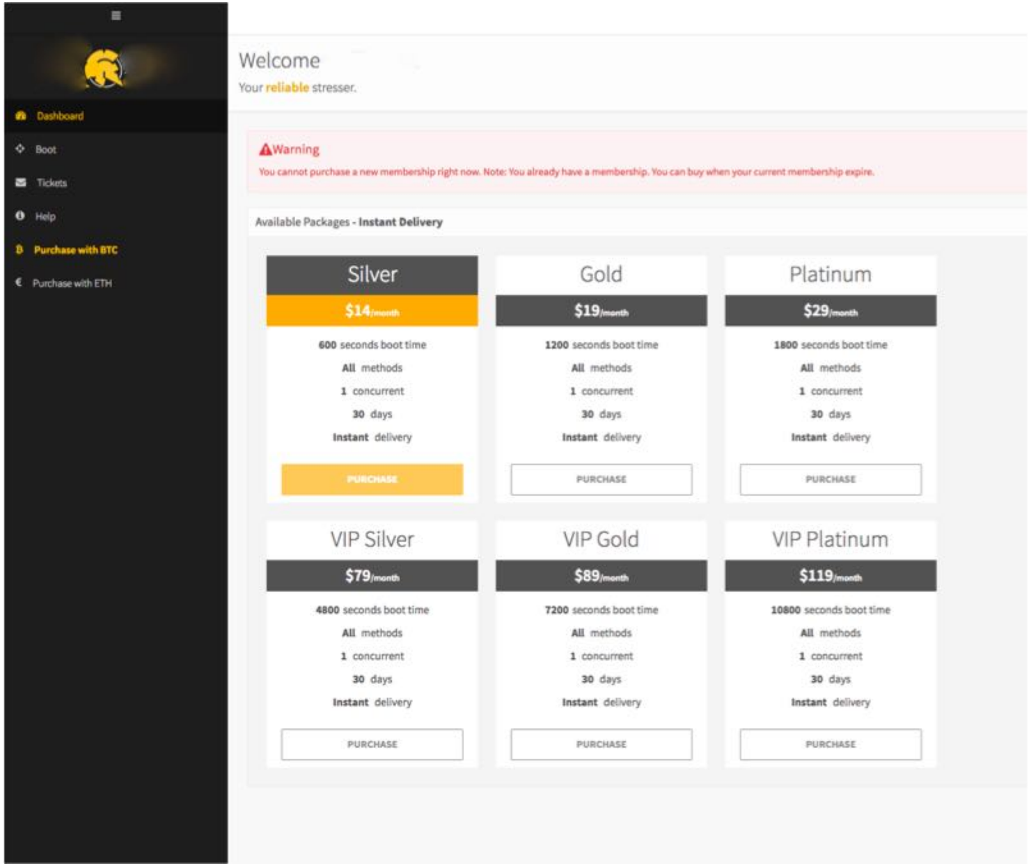
2602794

RUNING STRESS

42/96

DAILY STATISTICS

Example - Serviceplans



Welcome

Your reliable stresser.

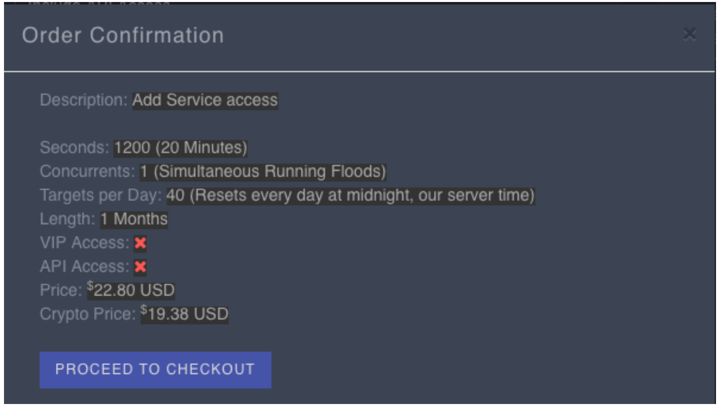
⚠Warning

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	**1200** seconds boot time	**1800** seconds boot time
All methods	**All** methods	**All** methods
1 concurrent	**1** concurrent	**1** concurrent
30 days	**30** days	**30** days
Instant delivery	**Instant** delivery	**Instant** delivery
PURCHASE	PURCHASE	PURCHASE

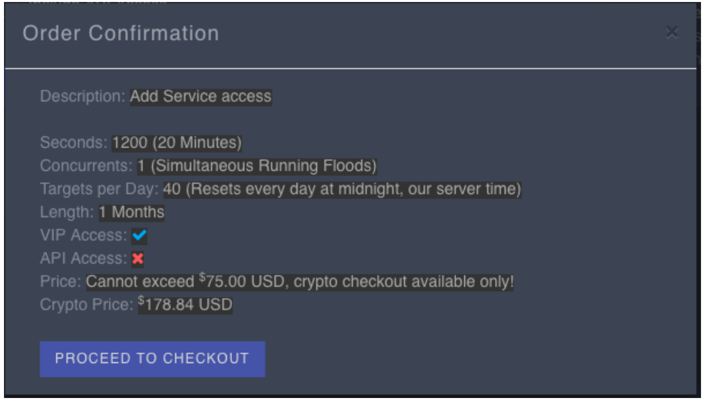
VIP Silver	VIP Gold	VIP Platinum
$79/month	$89/month	$119/month
4800 seconds boot time	**7200** seconds boot time	**10800** seconds boot time
All methods	**All** methods	**All** methods
1 concurrent	**1** concurrent	**1** concurrent
30 days	**30** days	**30** days
Instant delivery	**Instant** delivery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



Order Confirmation

Description: Add Service access

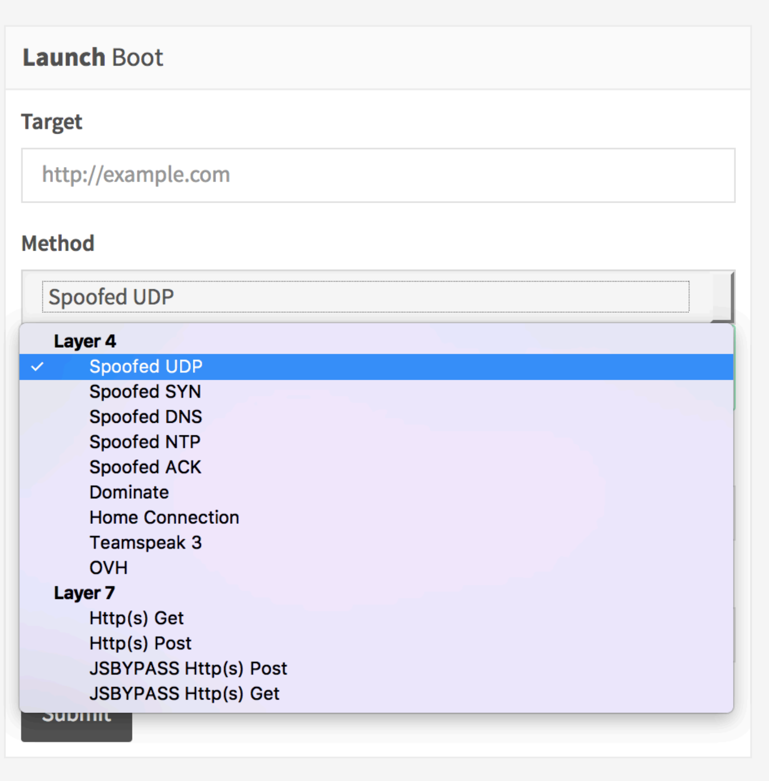
Seconds: 1200 (20 Minutes)
Concurrents: 1 (Simultaneous Running Floods)
Targets per Day: 40 (Resets every day at midnight, our server time)
Length: 1 Months
VIP Access: ✓
API Access: ✗
Price: Cannot exceed $75.00 USD, crypto checkout available only!
Crypto Price: $178.84 USD

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 bandwith

- Claim to offer
  5 - 100 Gbit/s



Launch Boot

Target

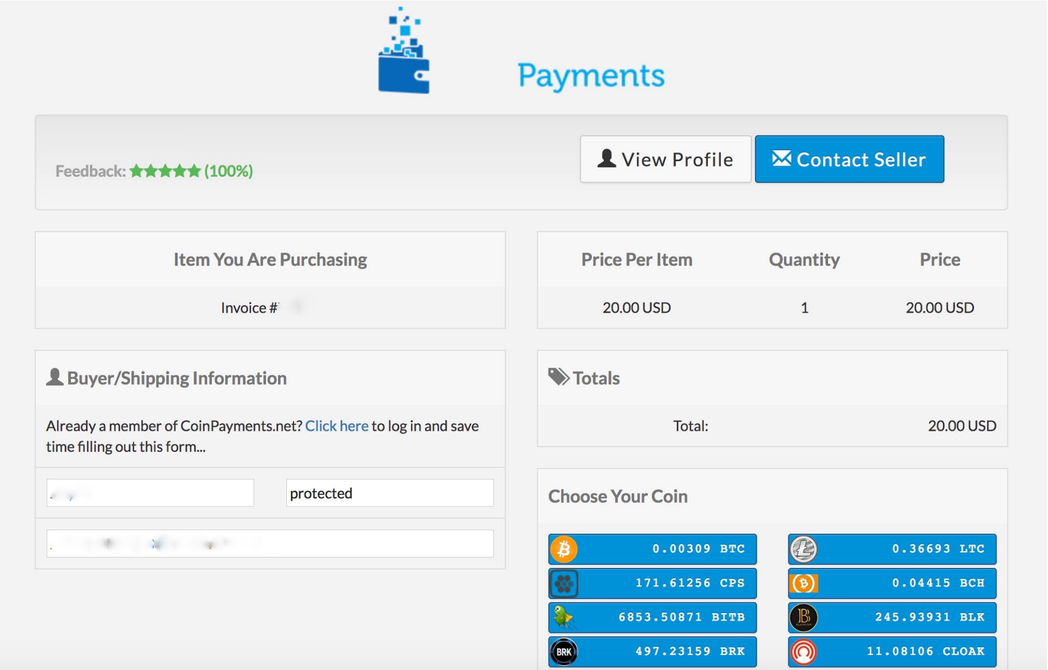
http://example.com

Method

Spoofed UDP

Payment

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



Feedback: ★★★★★ (100%)

Item You Are Purchasing
Invoice # [redacted]

Price Per Item	Quantity	Price
20.00 USD	1	20.00 USD

Buyer/Shipping Information

Already a member of CoinPayments.net? Click here to log in and save time filling out this form...

[redacted] protected

[redacted]

Totals

Total:	20.00 USD

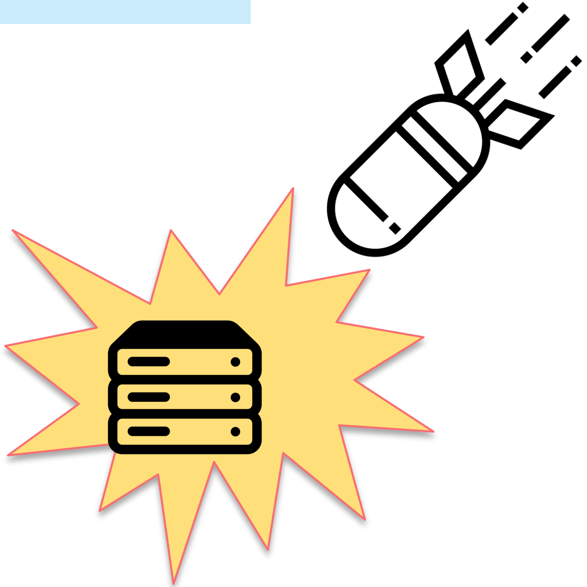
Choose Your Coin

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

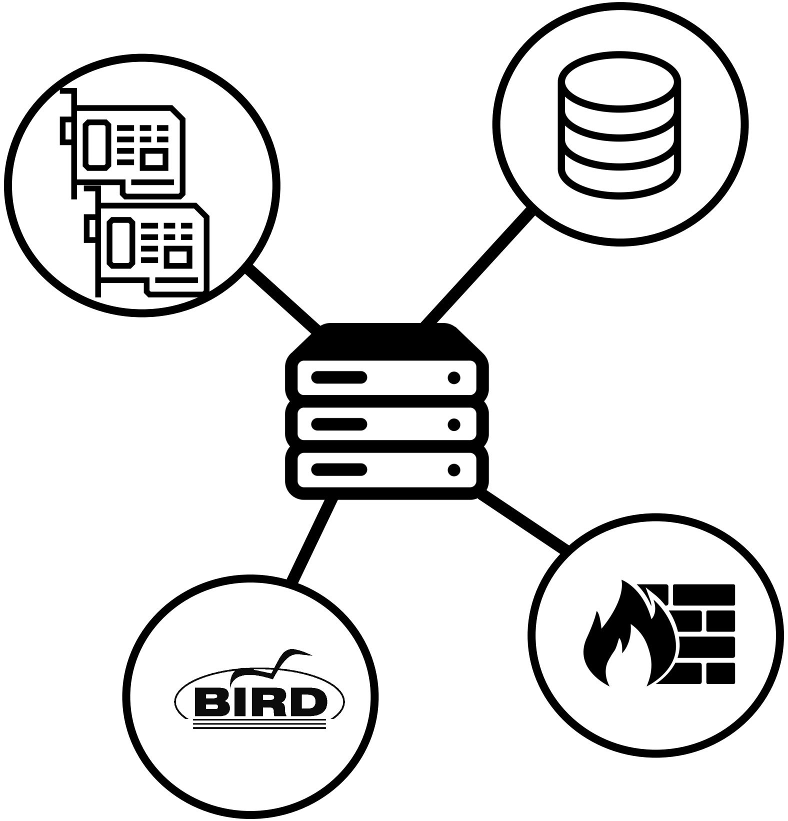
- **Requirements**
  - **Minimal impact during DDoS**
  - **Record 10 Gbit/sec to disc**
  - **Record at least continuous 30min**
  - **Global reachability**
  - **Direct connection to many ASNs**
  - **Keep costs low**



Measurement System and Setup

- Hardware
  - Dedicated second NIC as mirror
  - Fast write speed: SAS RAID-0
  - Dedicated Raid Controller
  - Singe core performance

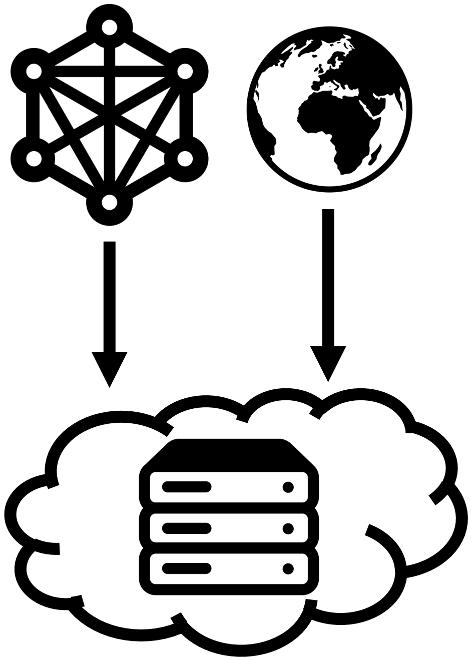
- System Setup
  - Linux as a BGP Router and Network
  - Bird & Docker
  - ARP! → ARP tables and IP tables



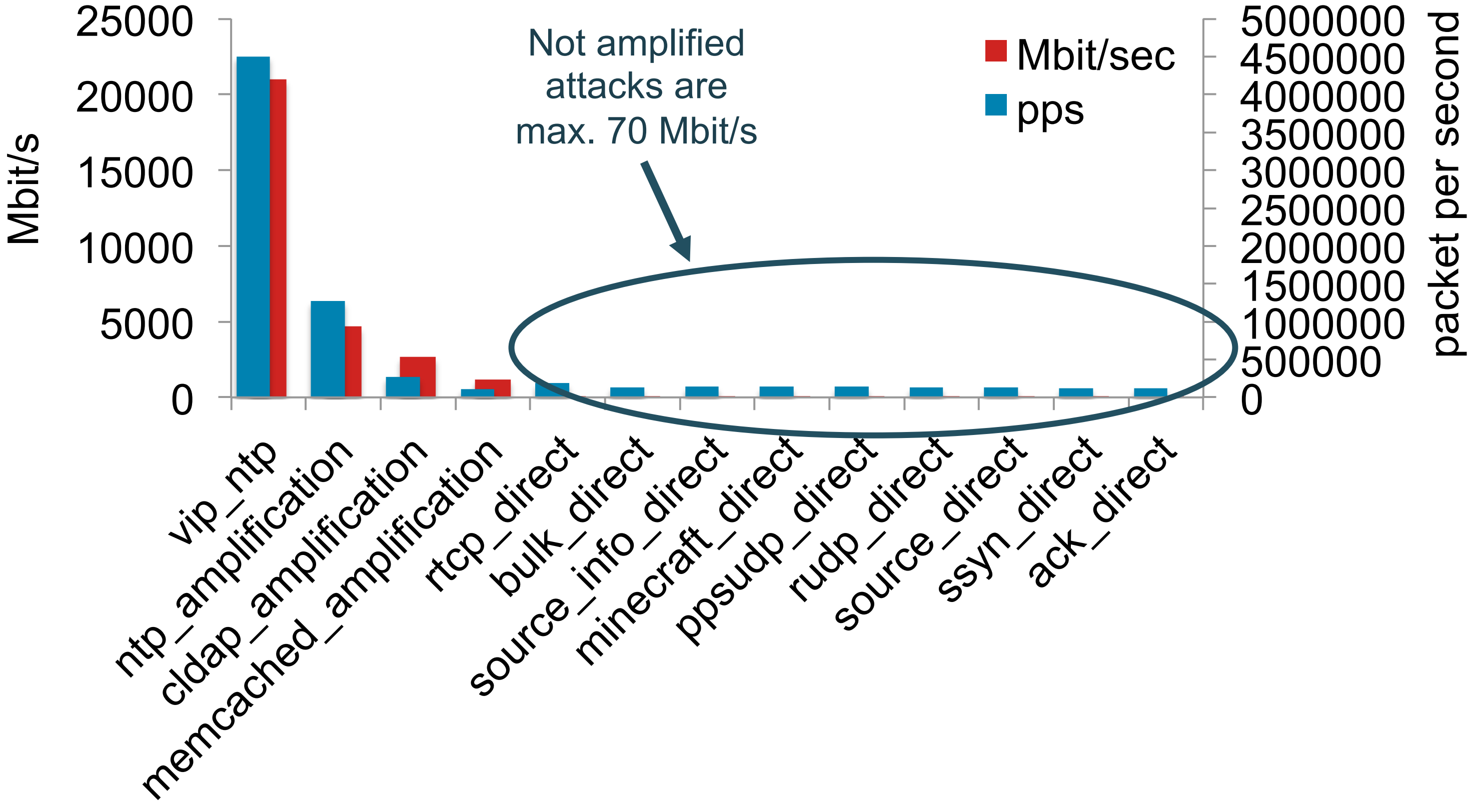
Measurement System and Setup

- Internet Connectivity
  - 10G Peering
  - 10G Transit
  - Own ASN and IPv4 Space

- Mesurement Limitations
  - Tcpdump → up to 10 Gbits/sec
  - sFlow → up to 10 Gbits/sec
  - IPFIX → over 100 GBit/secs



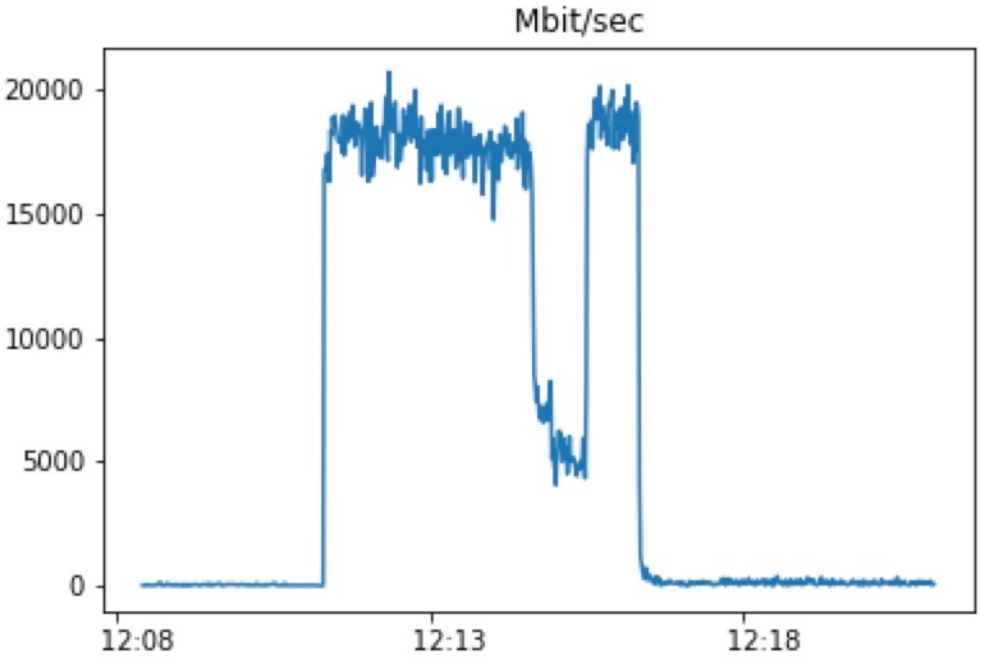
DDoS Attacks - Overview



Not amplified attacks are max. 70 Mbit/s

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

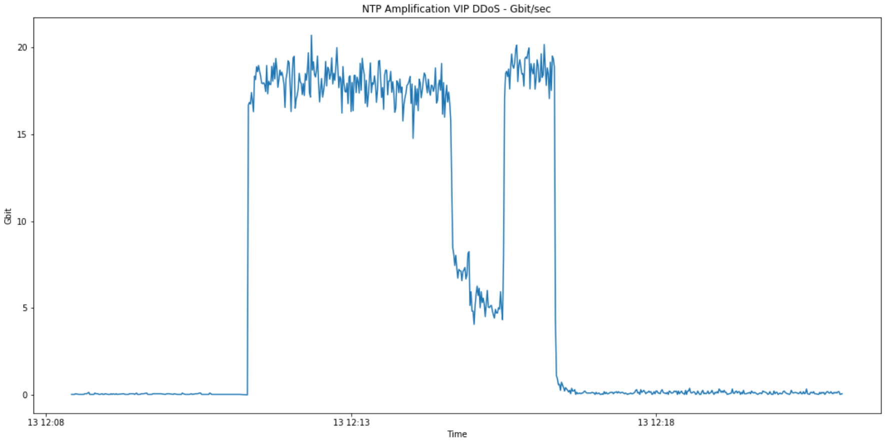


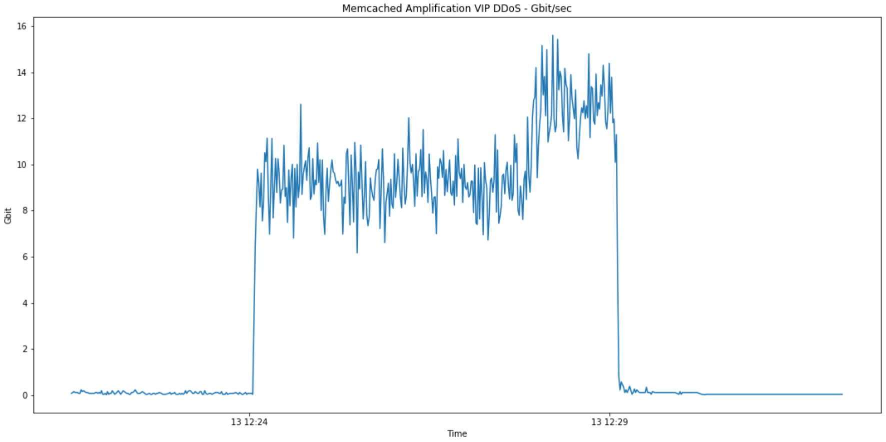
DDoS – NTP vs. Memchached Reflection

- **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**


NTP Amplification VIP DDoS - Gbit/sec


Memcached Amplification VIP DDoS - Gbit/sec

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

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

Q&A - Discussion - Feedback