RIPE 80
Virtual | 12 - 14 May

DDoS Hide and Seek – On the Effectivness of a Booter Service Takedown

D. Kopp[1], M. Wichtlhuber[1], I. Poese[2], J. Santanna[3], O. Hohlfeld[4], C. Dietzel[1,5]

DE-CIX[1], BENOCS[2], University of Twente[3], BTU[4], MPI[5]

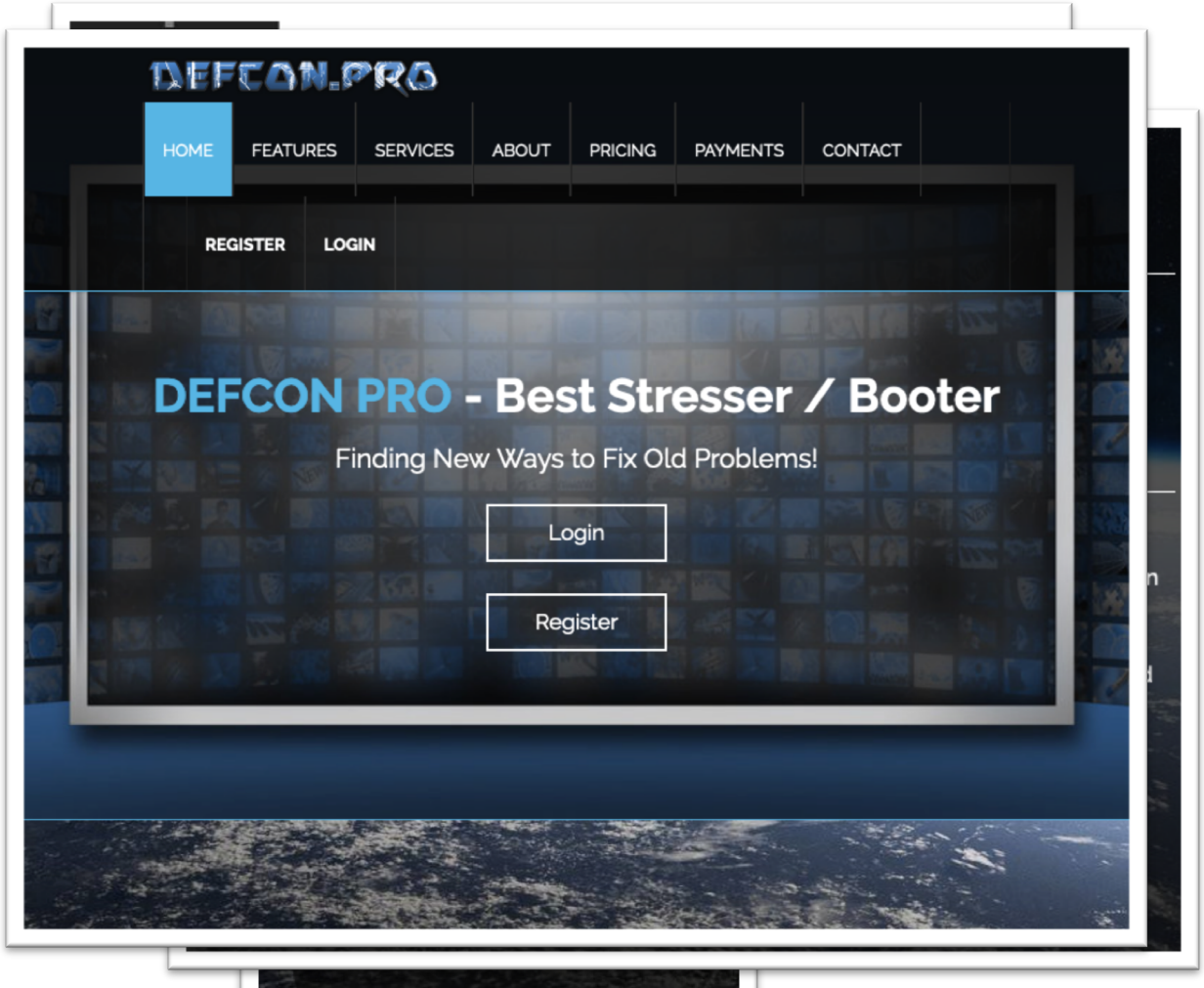
Booter Services

→ DDoS-as-a-service
- Web interface
- Easy to find and use

→ One klick to start a DDoS
- To any IP or domain

→ Pretend to be legal

→ Some offer service levels
- Payment in crypto cur.
- Usually 30 days flatrate



Attacks and Service Levels

→ 10 - 20 **different protocols (UDP, DNS..)**

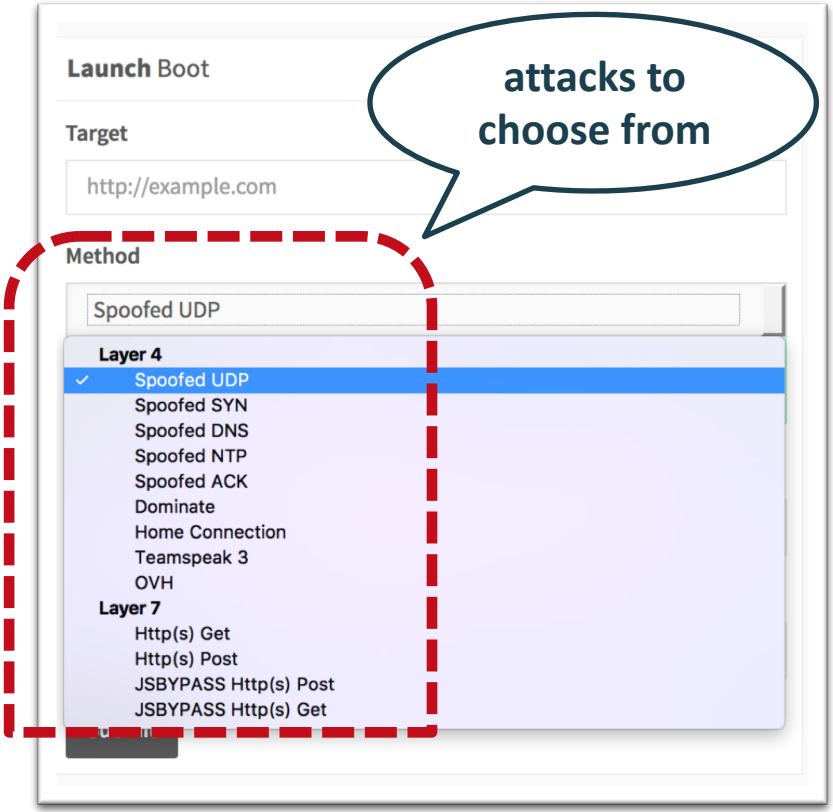
- Application → high pps
- Amplification → high bandwidth

→ Service plans differ by

- Number concurrent attacks
- Length of attacks

→ Claim to offer

- **5 - 12 Gbps basic less than 10$**
- **80 - 100 Gbps VIP more than 80$**



Take Down

FBI kicks some of the worst 'DDoS for hire' sites off the internet

Zack Whittaker

@zackwhittaker / 8:38 pm CET • December 20, 2018

Comment

Research Questions and Contribution

→ What's the threat of booter attacks?

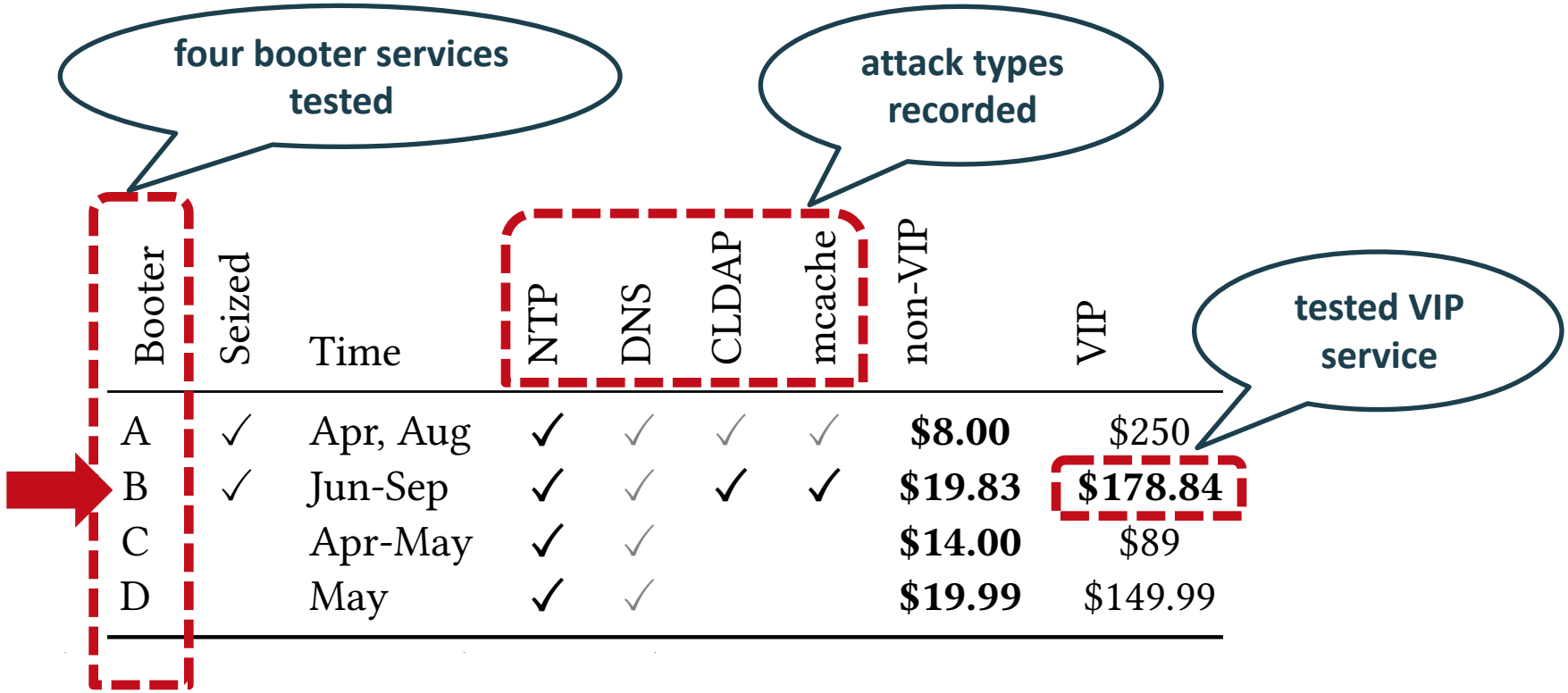
- Unique active measurement setup
- Anatomy and state of booter DDoS attacks
- Measurement of VIP DDoS

→ What's the state of DDoS attacks?

- NTP DDoS attacks at IXP, Tier-1 and Tier-2 ISP

→ What's the effect on attacks and traffic after the takedown of 15 booters?

Selection of Booter Services

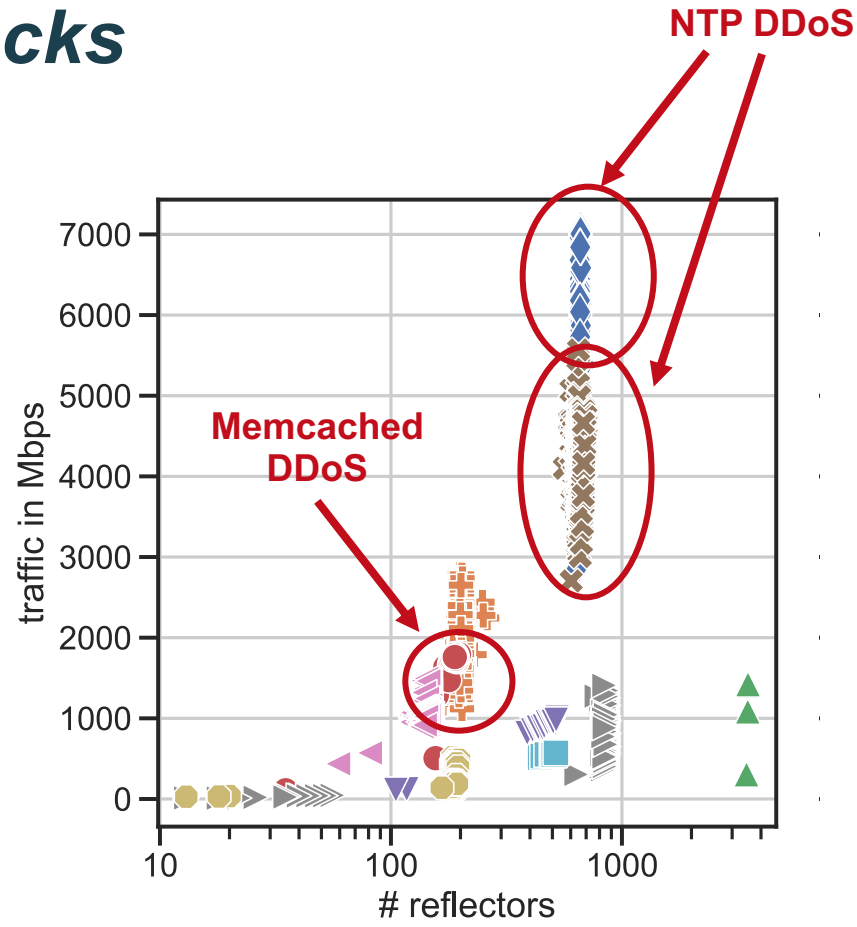


Booter	Seized	Time	NTP	DNS	CLDAP	mcache	non-VIP	VIP
A	✓	Apr, Aug	✓	✓	✓	✓	**$8.00**	$250
B	✓	Jun-Sep	✓	✓	✓	✓	**$19.83**	**$178.84**
C		Apr-May	✓	✓			**$14.00**	$89
D		May	✓	✓			**$19.99**	$149.99

Non-VIP Booter DDoS Attacks

- → 100 – 1000 reflectors
- → max. 7 Gbits
- → NTP attacks 80% via transit
- → Memcached 80% via IXP

- → **NTP attacks are the most significant attacks**



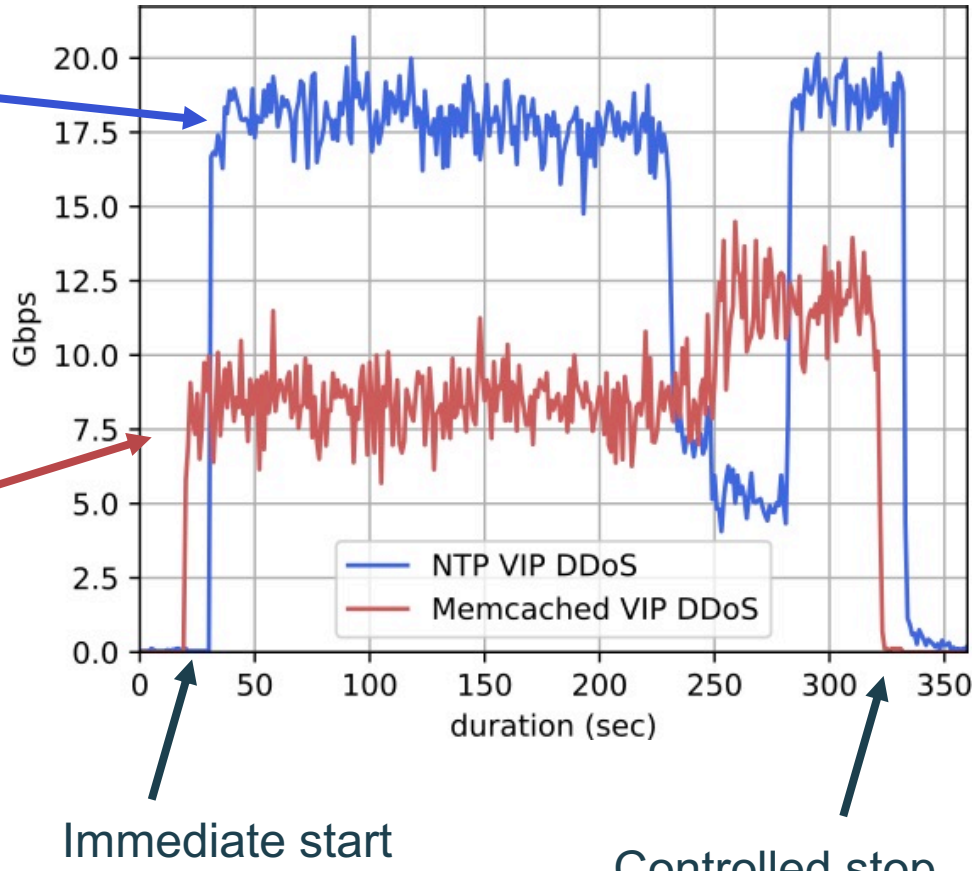
VIP Booter DDoS

→ NTP DDoS up to 20 Gbit/s

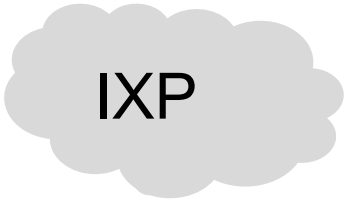
- 930 source IPs (reflectors)
- 350 source ASNs (networks)

→ Memcached DDoS up to 13 Gbit/s

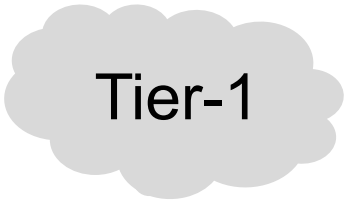
- NTP most significant attack



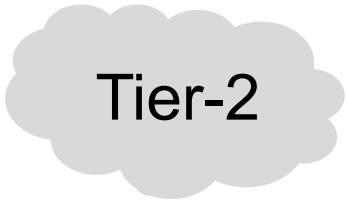
Passive Measurement Vantage Points



October 27 – January 31 (3.5 months)
834 Billion flows



December 12 – December 31 (3 weeks)
6.6 Billion flows

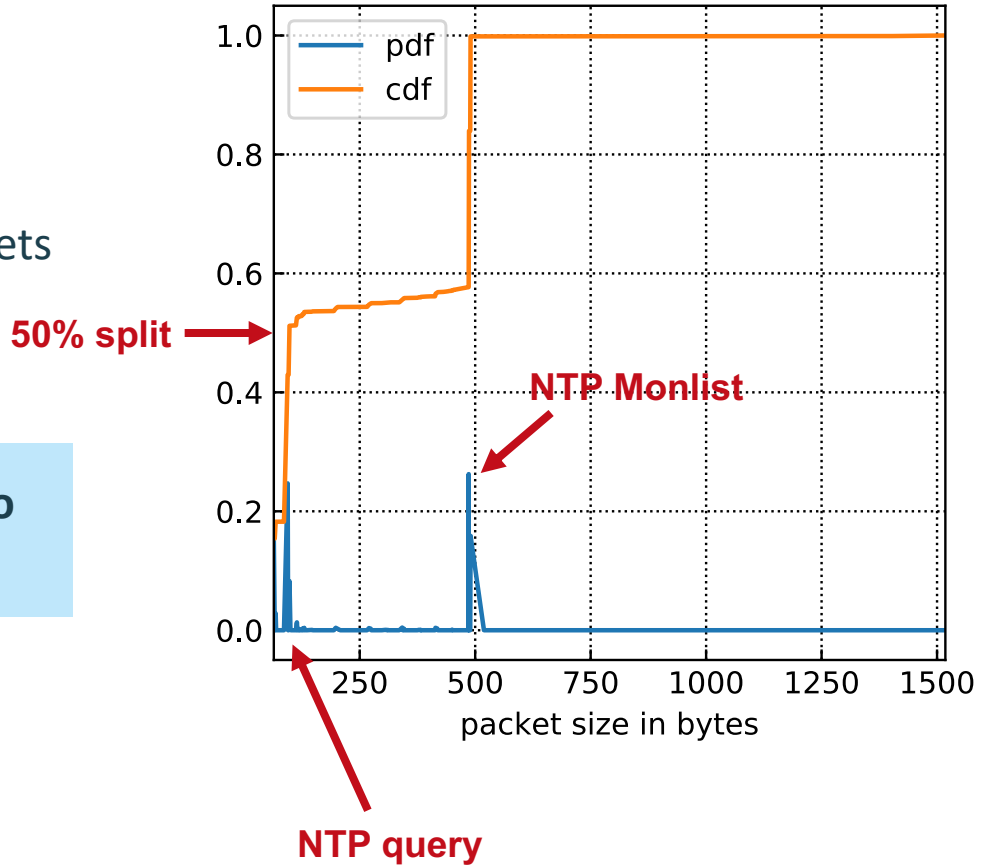


September 27 – February 2 (4.5 months)
470 Million flows

Distribution of NTP Packet Sizes

- → Small → NTP queries
- → Large → Monlist replies
- → Split at 50% for small and large packets

We use 200 bytes as a filter to find DDoS attacks



NTP DDoS Attacks in the Wild

→ We profile attack traffic

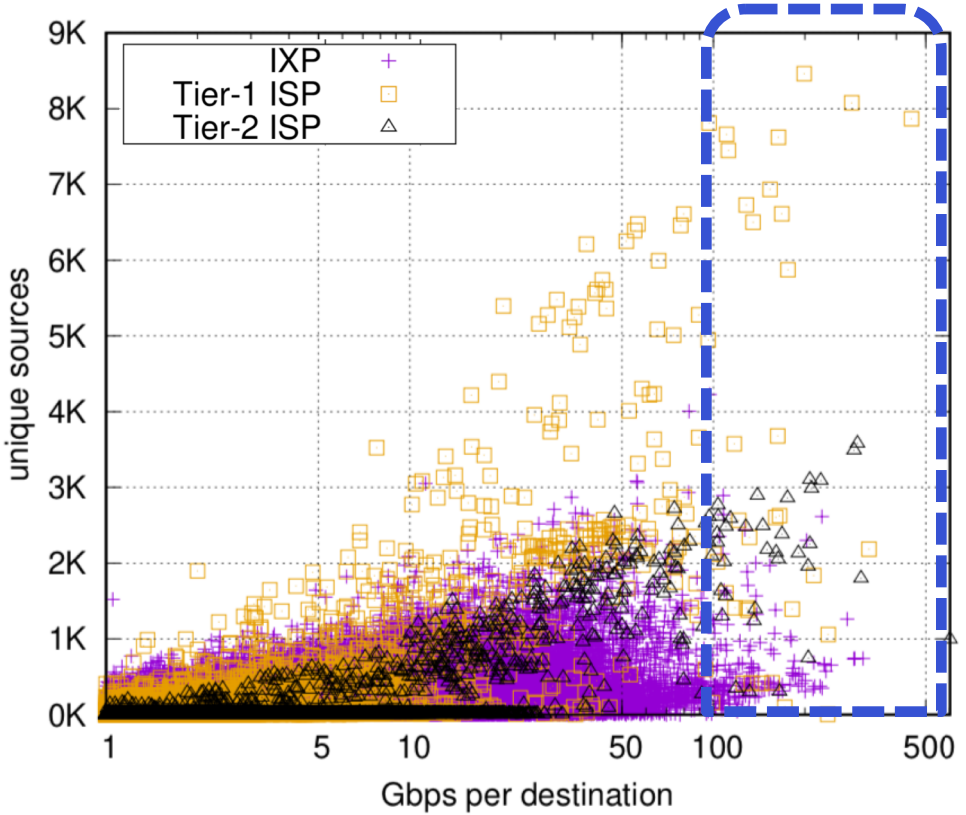
- Number of reflectors
- Max GBytes per second

→ 311K destinations

224 victims > 100 Gbps

5 > 300 Gbps

1 > 600 Gbps



NTP DDoS Attacks in the Wild – Anomalies

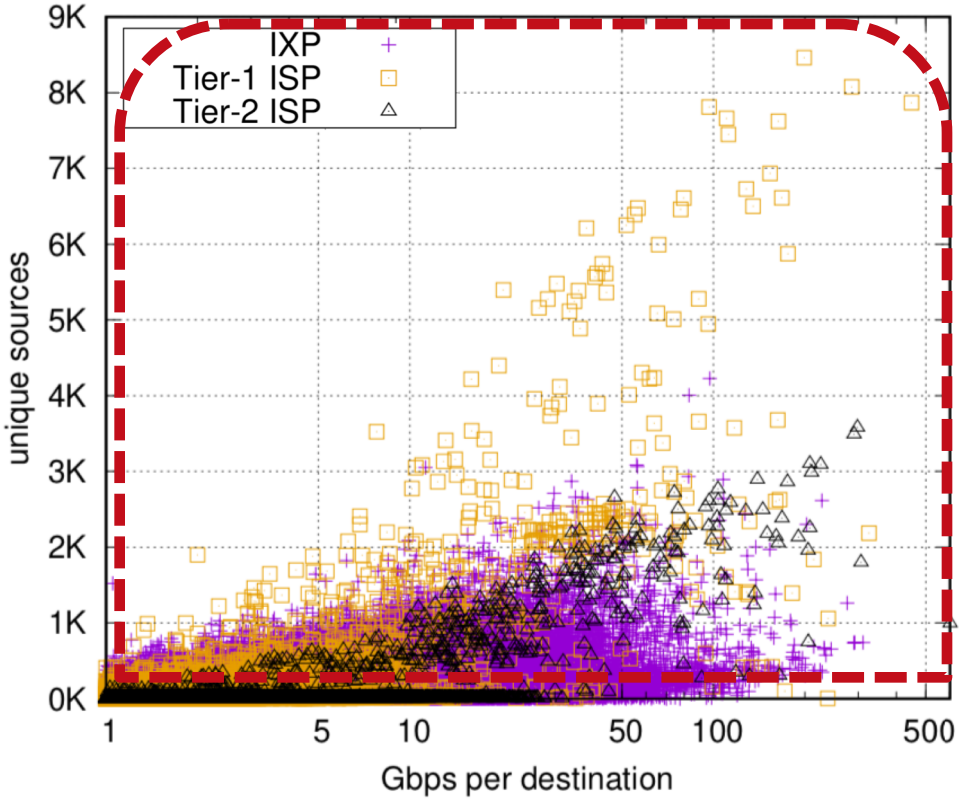
➔ Two filter criteria for **anomalies**:

1. Traffic > 1 Gbps
2. More than 10 sources

➔ Conservative filtering:

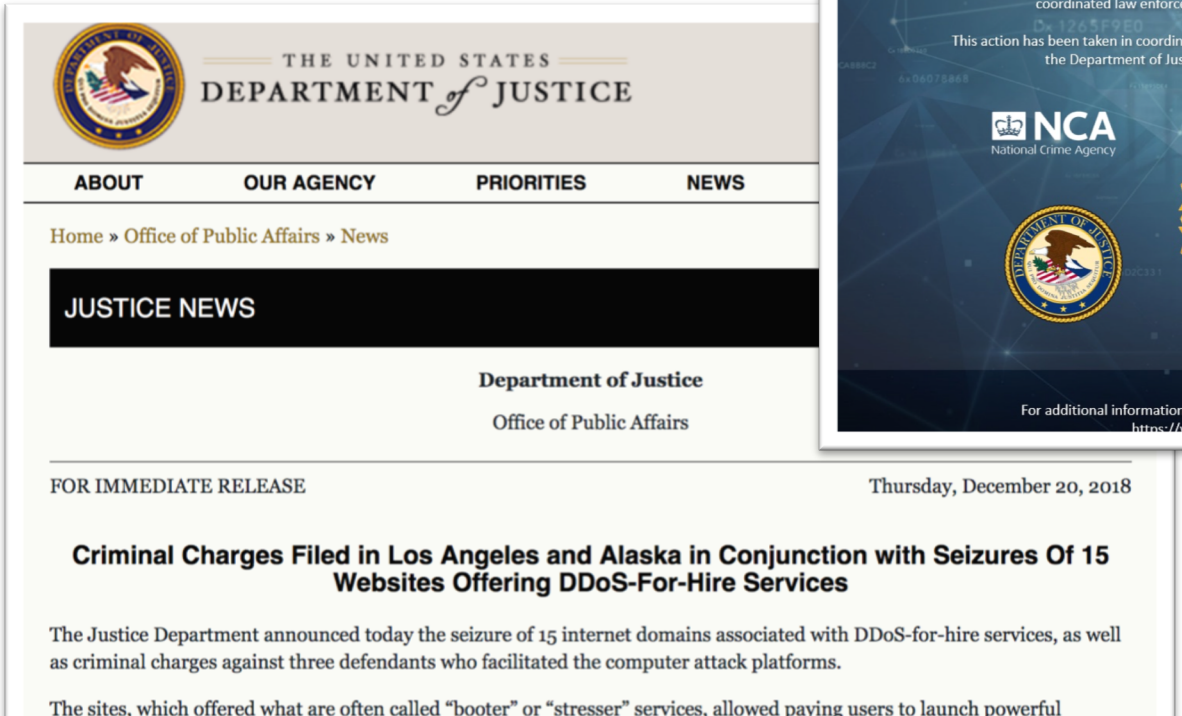
69k destinations

We use this filtering criteria to investigate attacks over time



Booter Services vs. FBI

→ FBI operation took down **prox. 15**
DDoS for hire services **Dec. 20, 2018**


THE UNITED STATES DEPARTMENT of JUSTICE

ABOUT OUR AGENCY PRIORITIES NEWS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

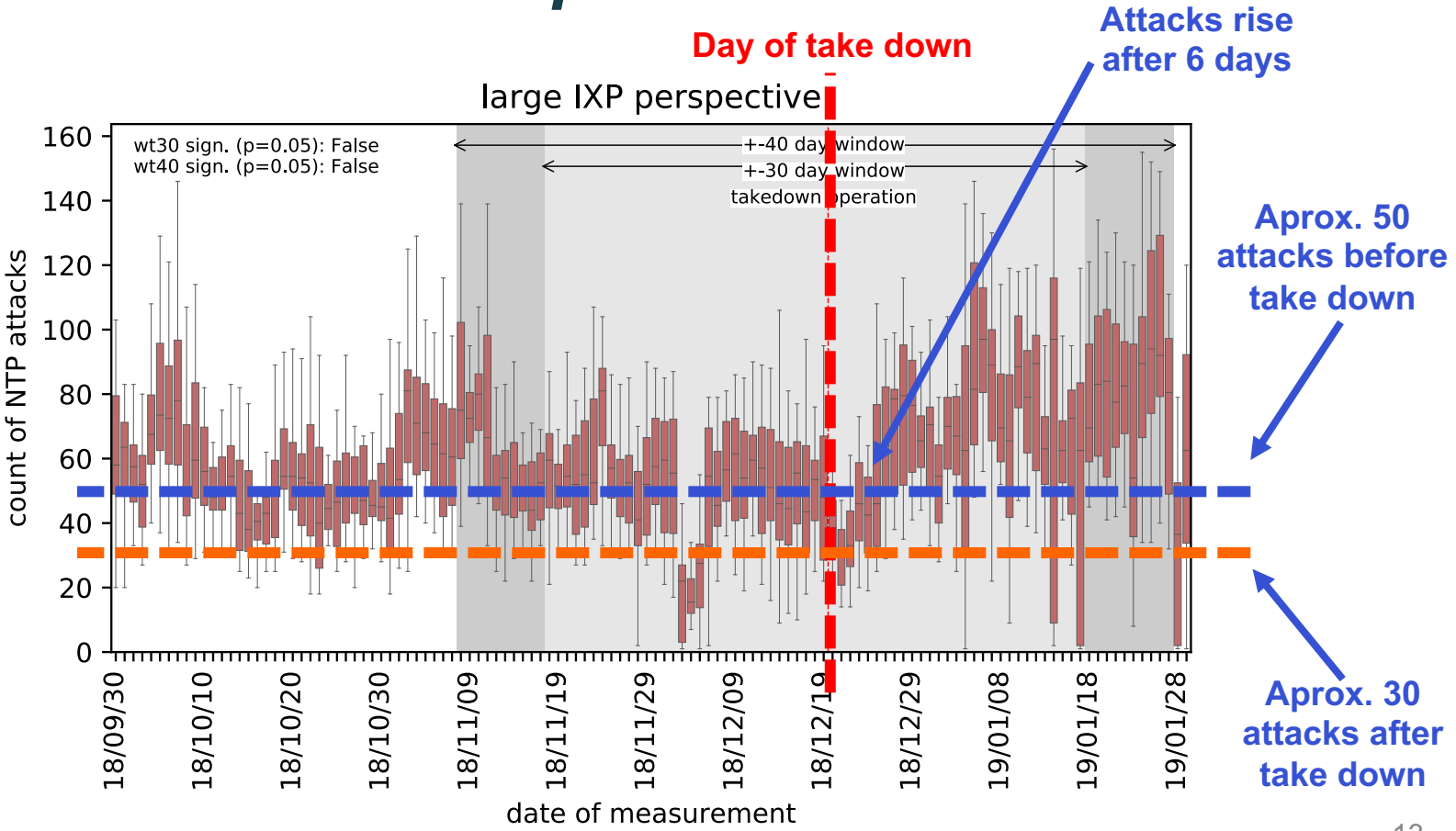
Thursday, December 20, 2018

Criminal Charges Filed in Los Angeles and Alaska in Conjunction with Seizures Of 15 Websites Offering DDoS-For-Hire Services

The Justice Department announced today the seizure of 15 internet domains associated with DDoS-for-hire services, as well as criminal charges against three defendants who facilitated the computer attack platforms.

The sites, which offered what are often called "booter" or "stresser" services, allowed paying users to launch powerful

IXP: NTP DDoS Attacks per Hour



Changes in DDoS Traffic

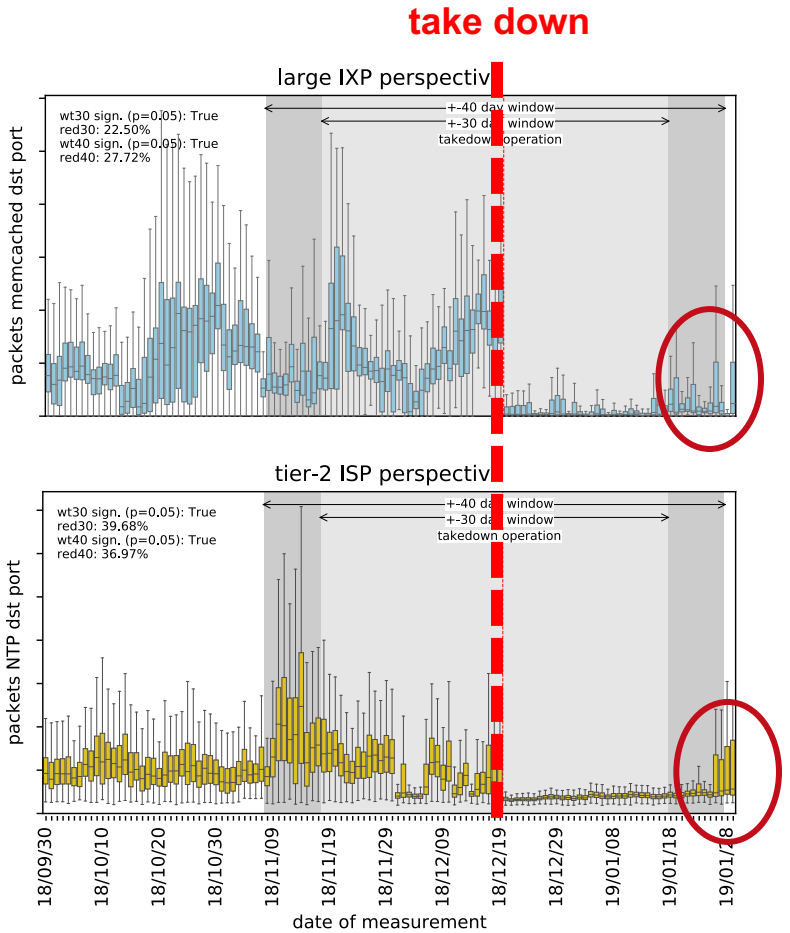
➔ Statistically significant changes
30/40 days around takedown

➔ We investigate NTP, DNS, Memcached

- IXP Memcached destination
- Tier-2 ISP NTP destination

➔ We find: Only traffic **towards reflectors** was affected

➔ **No significant changes in direct attack traffic**



Domain Perspective on FBI Takedown

➔ Data: weekly snapshots of all 140M .**com**/.**net**/.**org** domain

- DNS
- HTTPS

➔ Keyword search: “**booter**”, “**stresser**”, “**ddos-as-a-service**”, …
(following booterblacklist.com) [J. Santanna et. Al.]

➔ Search for new booter webpages and twins

Domain Perspective on FBI Takedown

→ Many **alternative** (non-seized) **booter sites exist** (58 for .com/.net/.org)

→ **Seized booter** appear popular, but **not the most popular** ones

→ Booter A **became active with a new domain** 2 days after seizure

- Domain registered in mid 2018
- Even our login credentials still work ;)

Conclusion

➔ Booters: user **friendly, cheap and popular** way to launch DDoS attacks

- You mostly get what you pay for but a lower bandwidth
- NTP DDoS attacks are the most potent
- Attacks size **citical** to most **small to medium networks**

➔ There is lots and permanent DDoS attack traffic in the Internet

➔ Law enforcement action in December 2018

- One booter became **active quickly after take down**
- Short-time reduction of requests to amplifiers
- Little effect on traffic reflected by amplifiers and attack count

Q&A - Discussion - Feedback