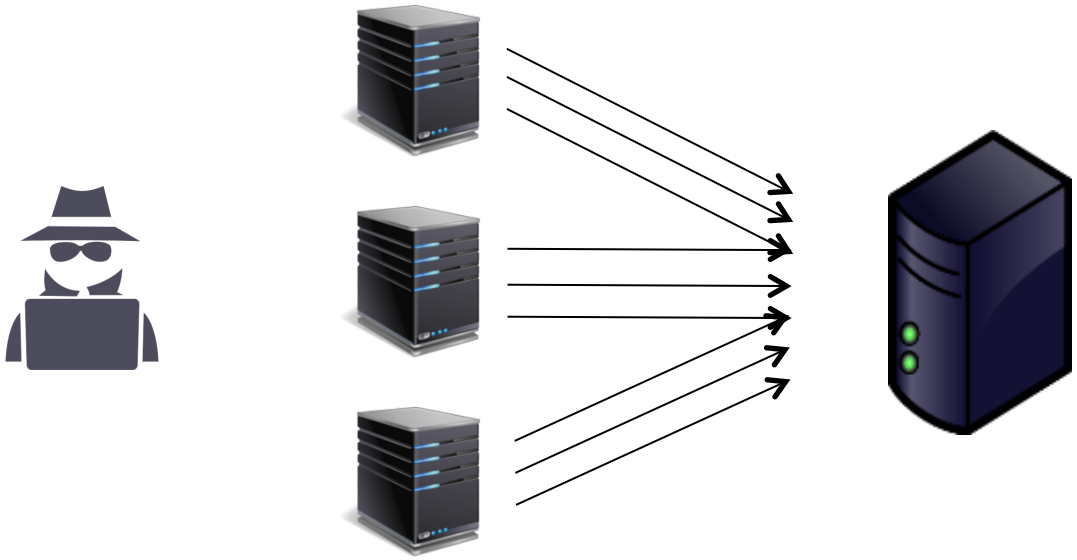
DDoS Hide & Seek: On the Effectiveness of a Booter Services Takedown

Oliver Hohlfeld

DE CIX UNIVERSITY OF TWENTE. BENOCS Brandenburg University of Technology Cottbus - Senftenberg

Overloading the Web Server



Distributed Denial of Service Attack

Performing DDoS Attacks

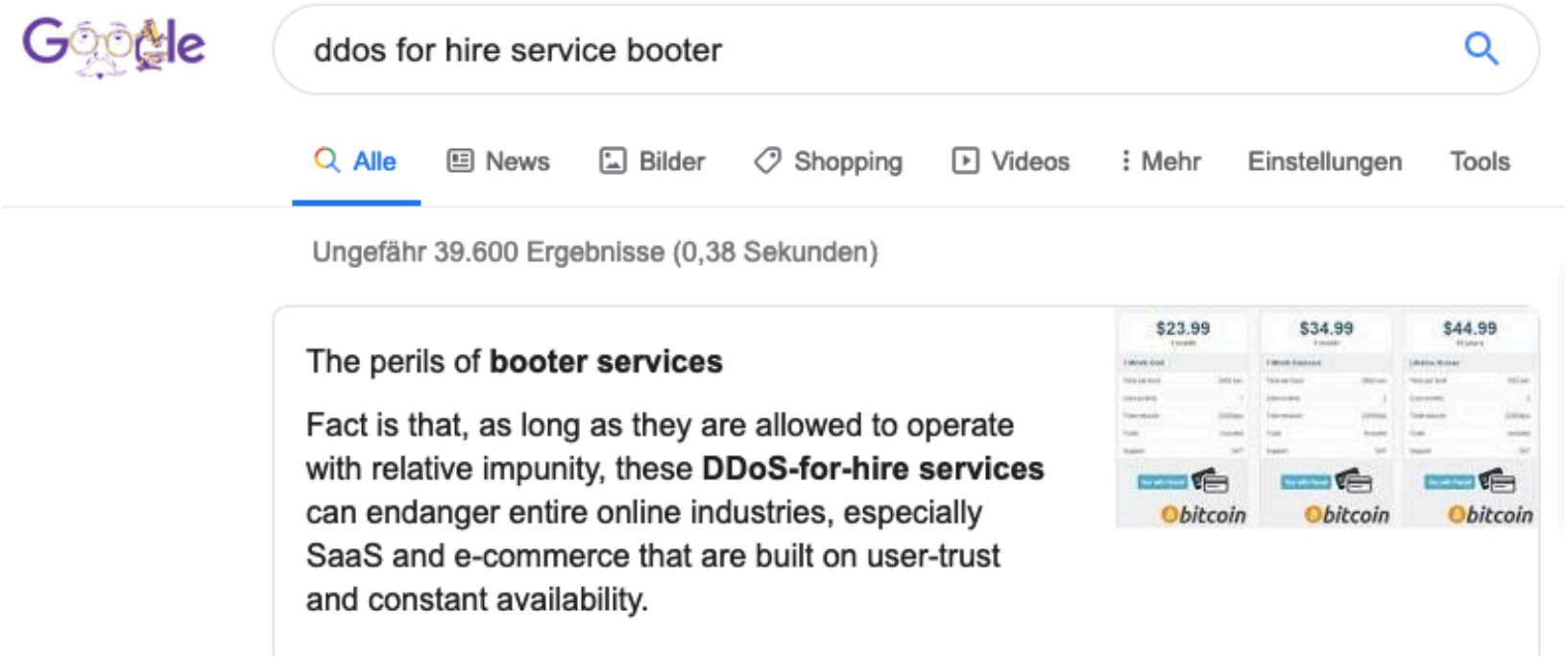
Requires

technical expertise

✔ infrastructure

→ Use somebody else's infrastructure
protocol flaws, unprotected systems, …

I am lacking expertise: let me Google it



[Demo]

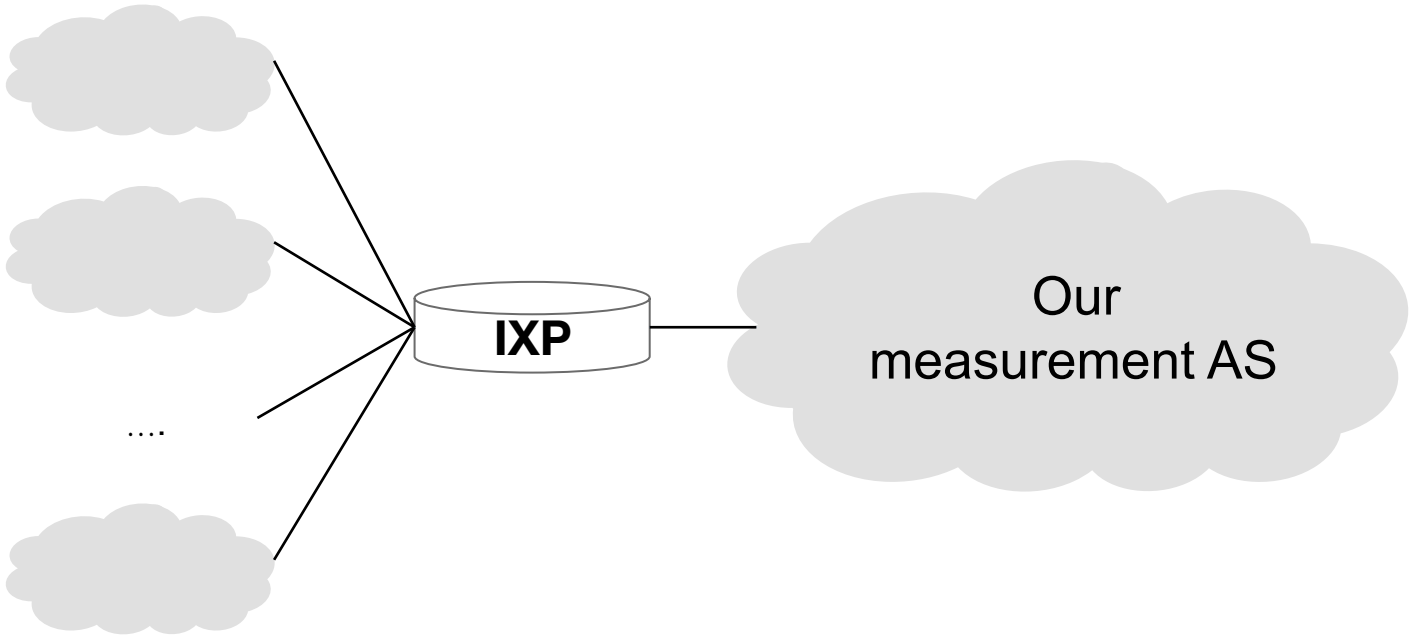
What is known about Booters

- Analysis of booter leaked customer databases
  [NM'15], [USENIX LEET'13]
- Victims: [Springer Attacks, Intrusions & Defenses'16]
- Booter blacklists & website fingerprinting
  [NM'18], [CNSM'16], [Collab. Comput. Conf.'18]
- Blacklist based booter market study
  [Commag'17]

Do they deliver what they promised?

Let's try to attack our own infrastructure

Measurement Infrastructure

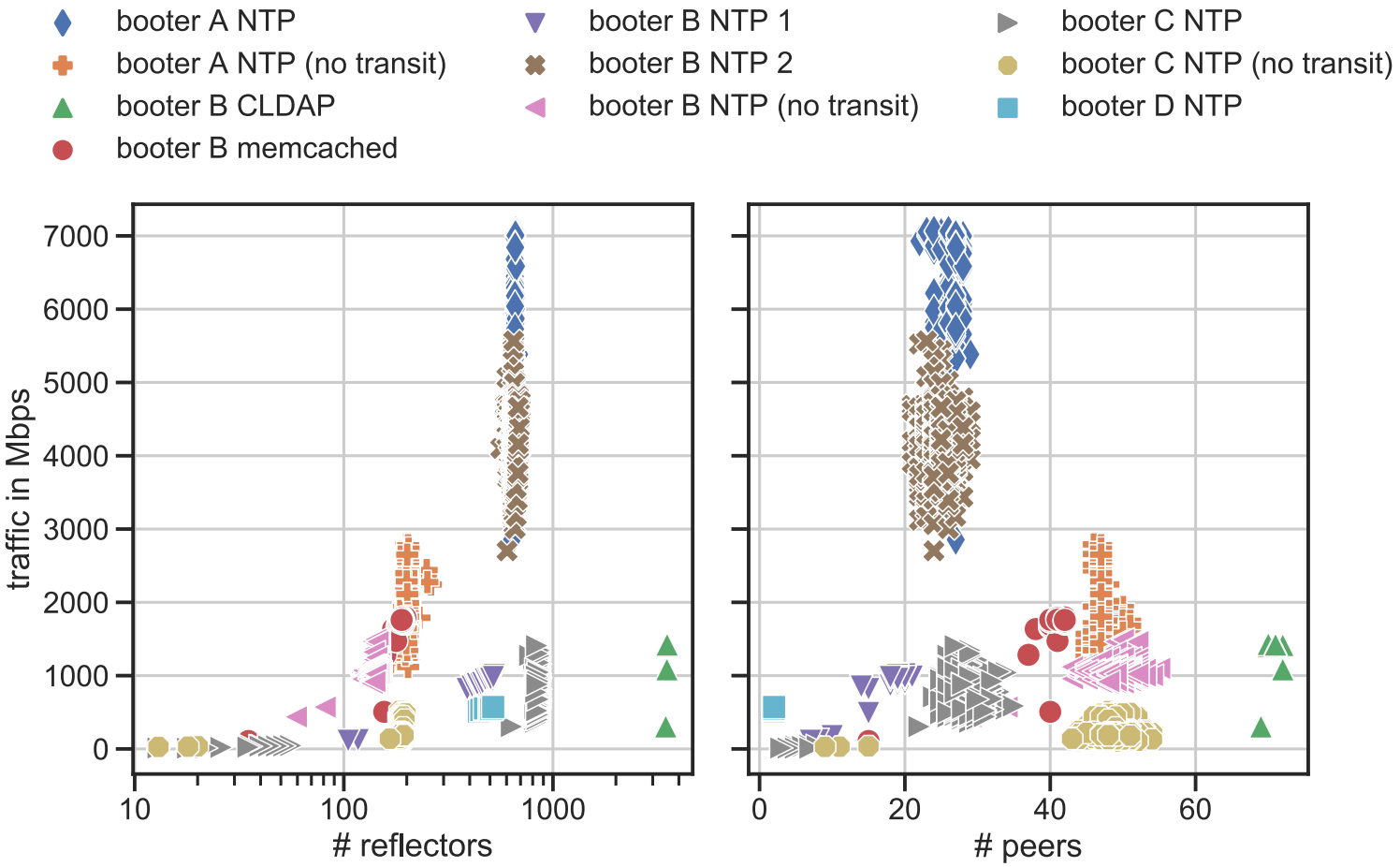


Buying Booter Services

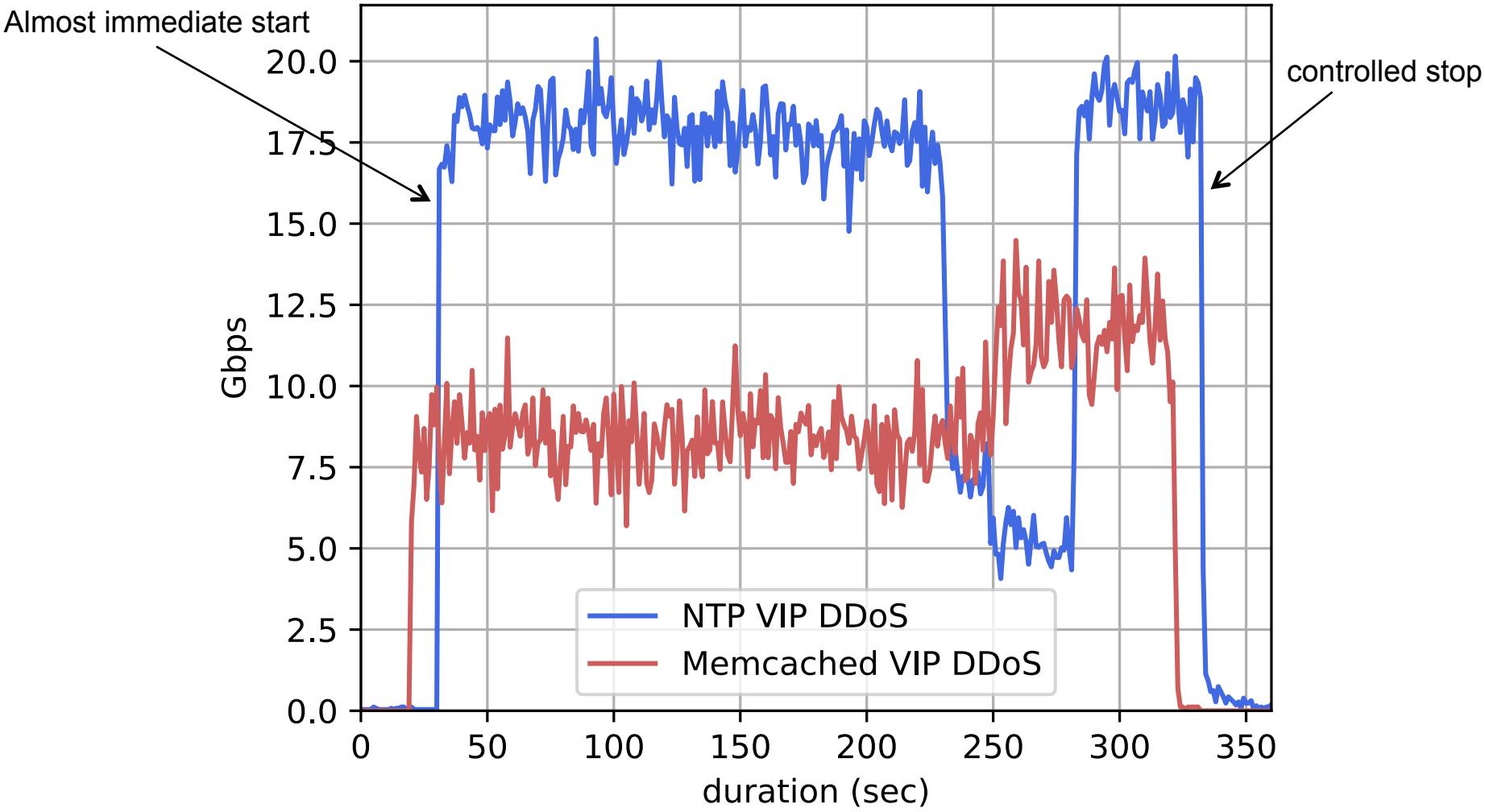
Booter	Seized	Time	NTP	DNS	CLDAP	mcache	non-VIP	VIP
A	✓	Apr, Aug	✓	✓	✓	✓	**$8.00**	$250
B	✓	Jun-Sep	✓	✓	✓	✓	**$19.83**	**$178.84**
C		Apr-May	✓	✓			**$14.00**	$89
D		May	✓	✓			**$19.99**	$149.99

- Booter B offers:
  - Cheaper non-VIP services: 8-12 Gbps
  - More expensive VIP services: 80-100 Gbps

Cheaper, non VIP Services



More expensive, VIP services



It works

We’re not the only ones knowing that

December 2018

15 booter domains

THIS WEBSITE HAS BEEN SEIZED

This domain has been seized by the Federal Bureau of Investigation pursuant to a seizure warrant issued by the United States District Court for the Central District of California under the authority of 18 U.S.C. §1030(i)(1)(A) as part of coordinated law enforcement action taken against illegal DDoS-for-hire services.

This action has been taken in coordination with the United States Attorney's Office of the District of Alaska, the Department of Justice Computer Crime and Intellectual Property Section, and

NCA National Crime Agency

POLITIE

For additional information, see the FBI Public Service Announcement I-101717b-PSA, https://www.ic3.gov/media/2017/171017-2.aspx

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

Zack Whittaker

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

Comment

The FBI has seized the domains of 15 high-profile distributed denial-of-service (DDoS) websites after a coordinated effort by law enforcement and several tech companies.

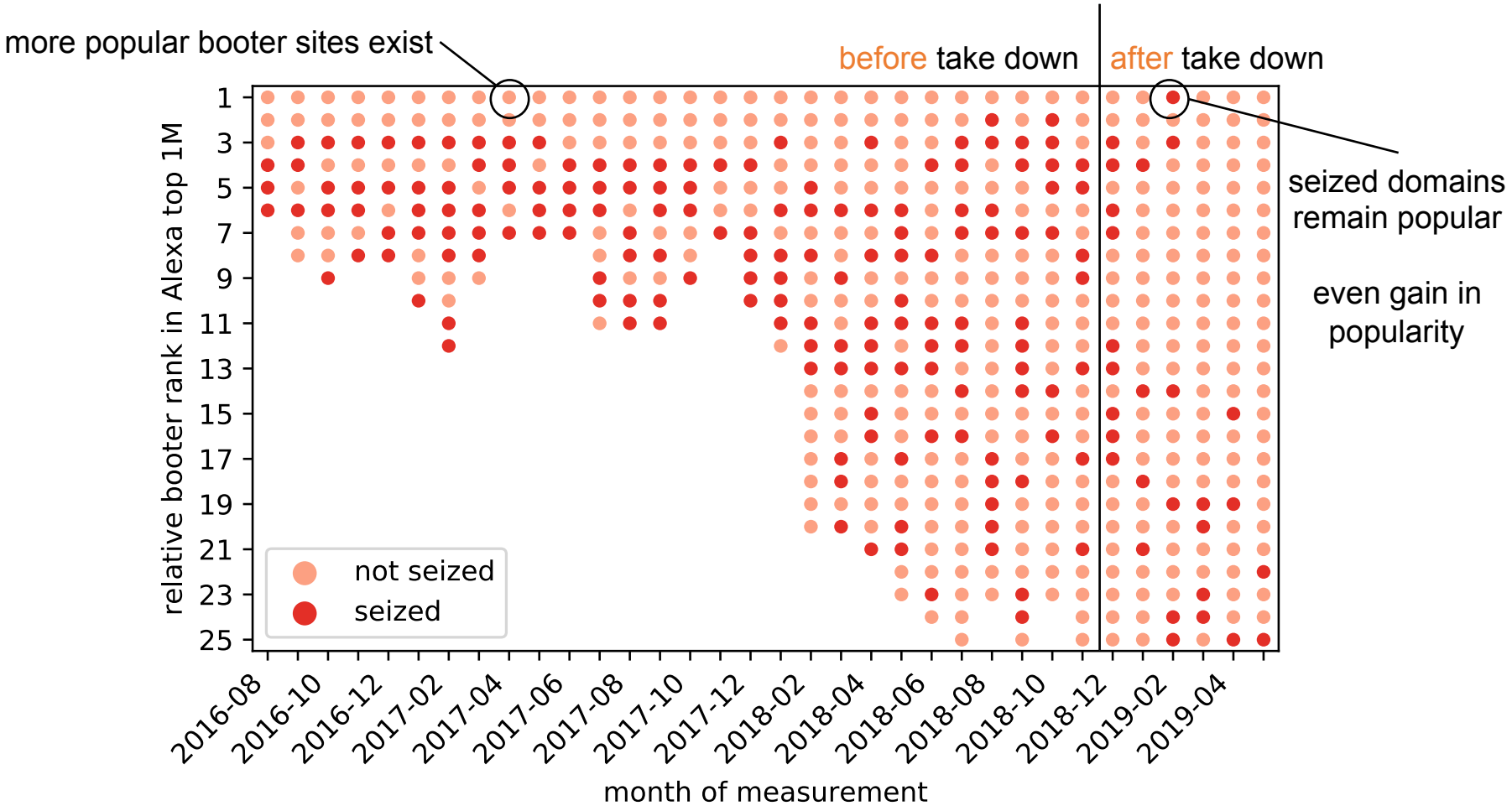
Domain Perspective on FBI Takedown

- Data: weekly snapshots of all 140M .com/.net/.org domain
  - DNS
  - HTTPS
  - August 2016 – April 2019

- Keyword search: “booter”, “stresser”, “ddos-as-a-service”, … (following booterblacklist.com)

- →Many alternative (non-seized) booter sites exist

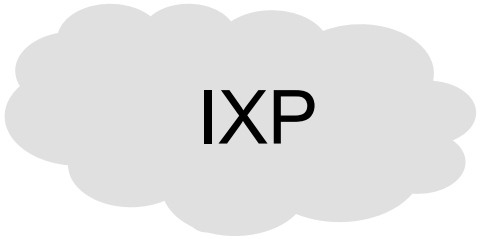
Popularity of Seized Booter Websites



Seized booter papers popular, but not the most popular ones

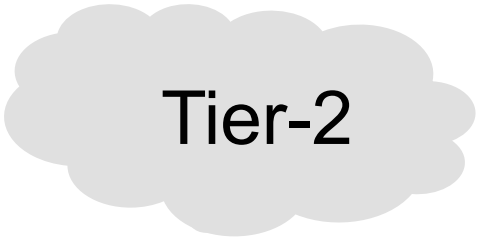
Did this takedowns had any effect?

Vantage Points



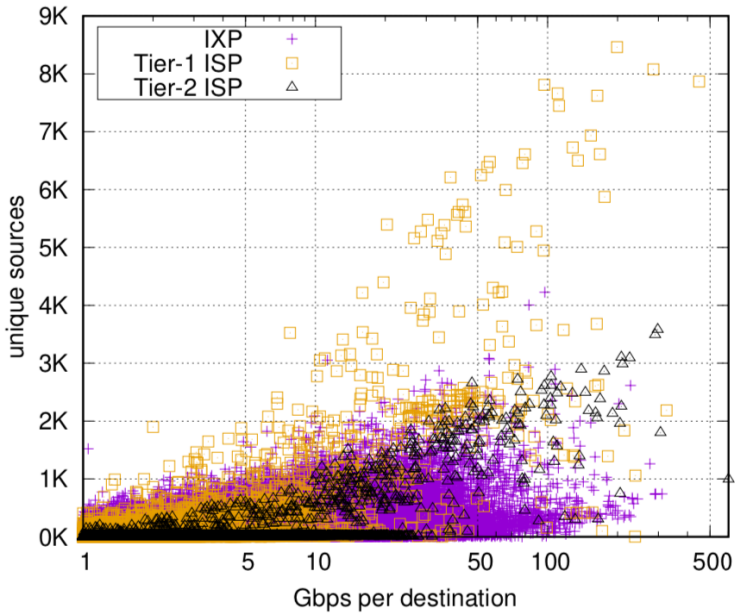
October 27 – January 31
834 B flows

December 12 – December 31
6.6 B flows



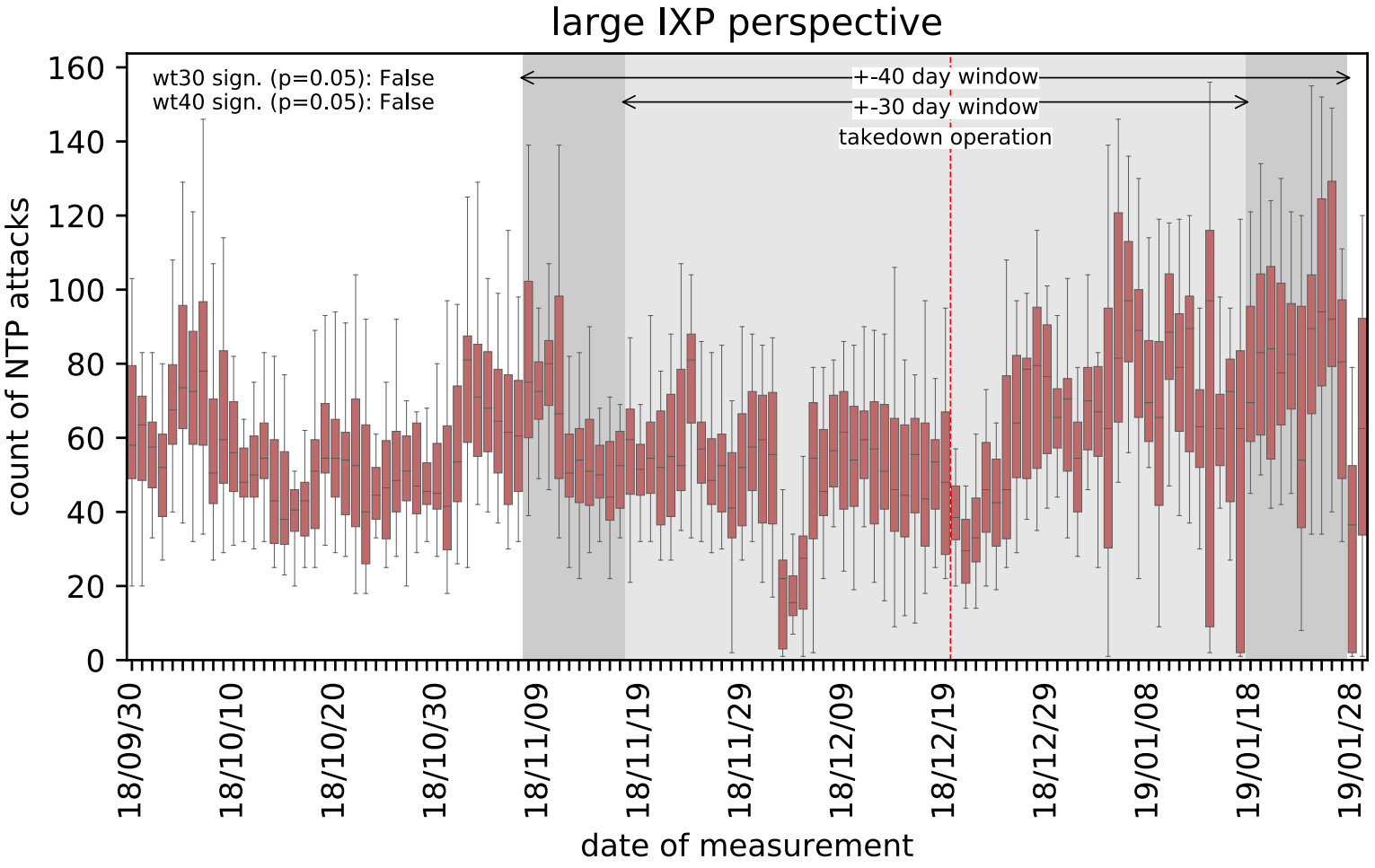
September 27 – February 2
470 M flows

NTP DDoS Attacks in the Wild



- 311K destinations (Tier-1 ISP: 36K , Tier-2 ISP: 95K , IXP: 244K) that receive NTP reflection traffic
- Conservative filtering / view: 69k destinations
- 224 victims receives > 100 Gbps,
  5 > 300 Gbps
  1 > 600 Gbps

IXP: Systems under NTP DDoS attack per hour



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)
- Many alternative (non-seized) booter sites exist
- Booter A became active with a new domain 2 days after seizure
  - Domain registered in mid 2018
  - Even our login credentials still work ;)

Conclusions

- Booters: user friendly and cheap way to launch DDoS attacks
  - You mostly get what you pay for
- There is lots of DDoS attack traffic in the Internet
- Law enforcement action in December 2018 had little success
  - One booter became active quickly after take down
  - Short-time reduction of requests to amplifiers
  - No effect of take down on attack traffic reflected by amplifiers

ARTIFICIAL INTELLIGENCE-BASED IXP DDOS MITIGATION
BMBF 2019 – 2022
DE-CIX & BTU