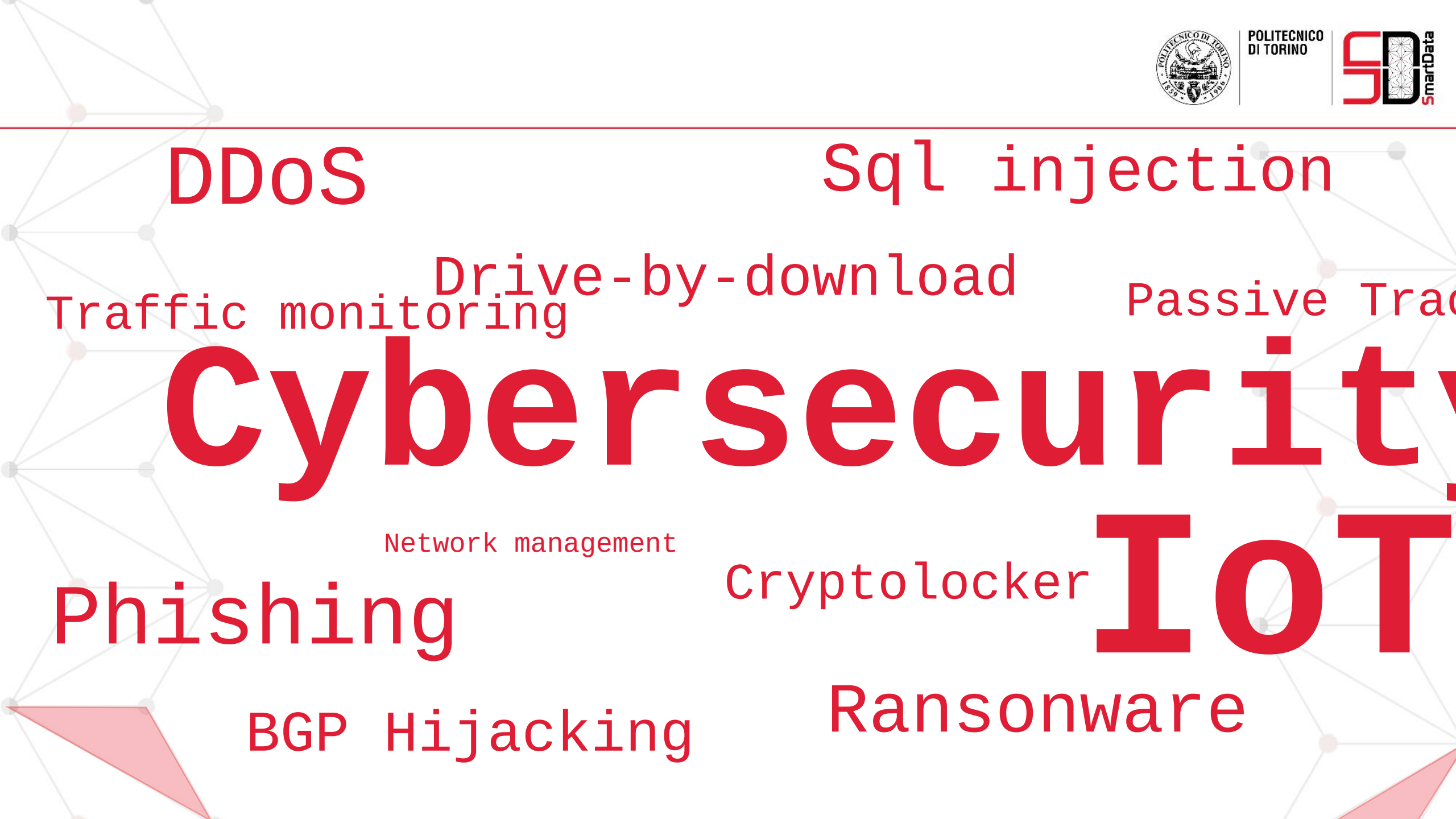
Darknets for Security Monitoring @ Polito

Idilio Drago
SmartData@PoliTo
https://smartdata.polito.it


DDoS
Sql injection
Drive-by-download
Traffic monitoring
Passive Trac
Cybersecurity
IoT
Network management
Cryptolocker
Phishing
Ransonware
BGP Hijacking

SmartData@PoliTo

Collect Data

- Active crawling
  - Web pages
  - Social networks (FB, Instagram, tripadvisor…)
- Passive probes
  - Up to 100 Gb/s with off-the-shelf hw
  - 5+ years of historical logs from ISP and campus networks
- Darknets
  - From 2 different countries
- Hon

Process Data

- Supervised ML
  - trees, forests, NN, GAN,…
  - For traffic classification
  - For malware detection
  - For user characterization
  - …
- Unsupervised ML
  - Clustering, Rule Mining
  - For anomaly detection
  - For lowering complexity
  - …

Solve problems

- System characterization
  - How does [dropbox|Skype|YouTube|…] work?
- User Characterization
  - How does Alice use [Dropbox|Instagram|YouTube]?
- Cybersecurity
  - How does Trudy abuse of [DNS, servers, cloud, news…]

Generation → Acquisition → Storage → Analysis

SmartData@PoliTo

Collect Data

- Active crawling
  - Web pages
  - Social networks (FB, Instagram, tripadvisor…)
- Passive probes
  - Up to 100 Gb/s with off-the-shelf hw
  - 5+ years of historical logs from ISP and campus networks
- Darknets
  - From 2 different countries
- Hon

Process Data

- Supervised ML
  - trees, forests, NN, GAN,…
  - For traffic classification
  - For malware detection
  - For user characterization
  - …
- Unsupervised ML
  - Clustering, Rule Mining
  - For anomaly detection
  - For lowering complexity
  - …

Solve problems

- System characterization
  - How does [dropbox|Skype|YouTube|…] work?
- User Characterization
  - How does Alice use [Dropbox|Instagram|YouTube]?
- Cybersecurity
  - How does Trudy abuse of [DNS, servers, cloud, news…]

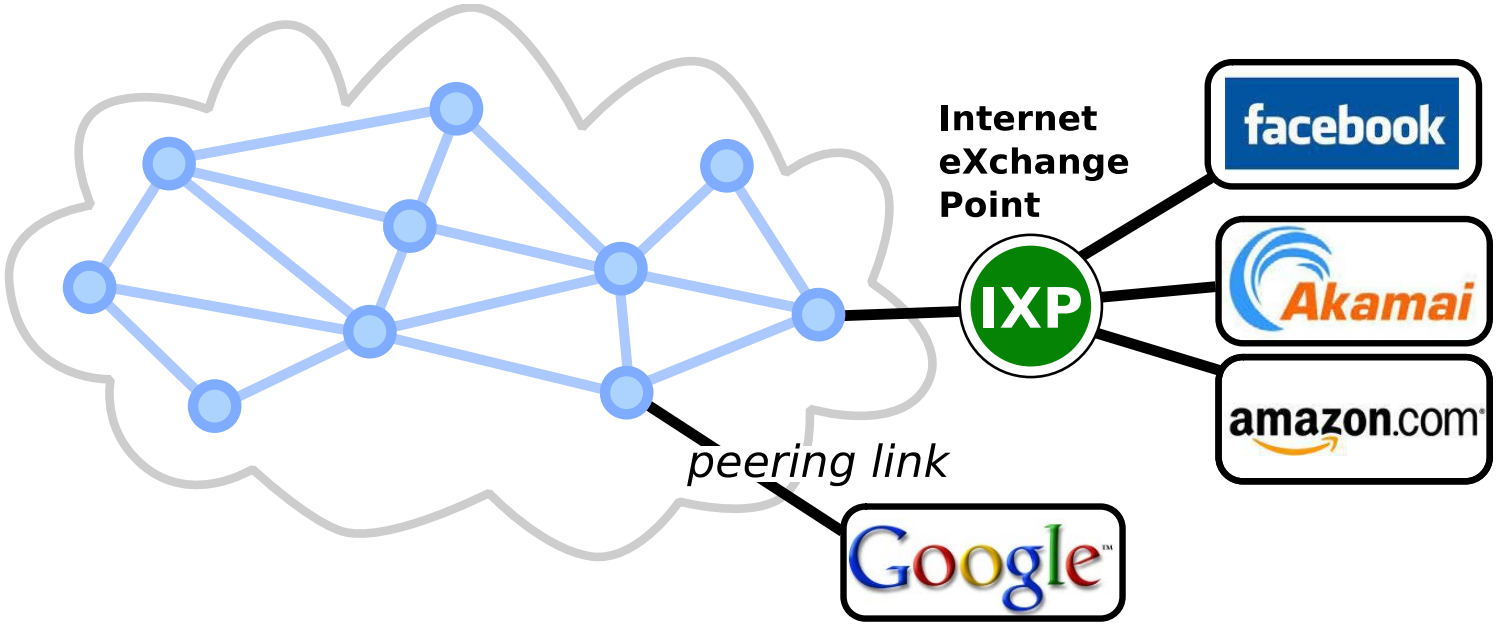
Generation

is

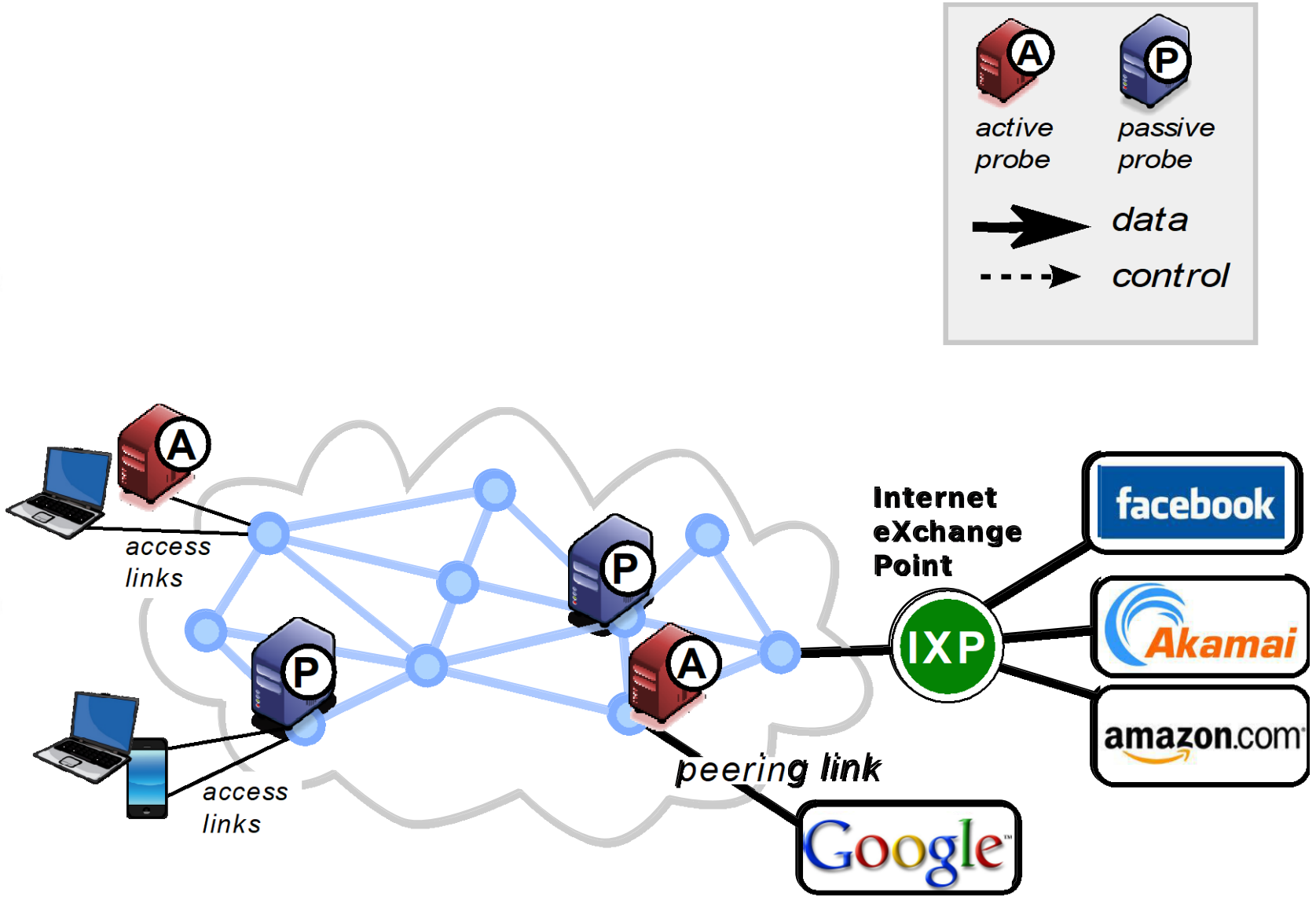
GOAL: make it as **automatic** as possible

Internet Traffic Monitoring @ Polito

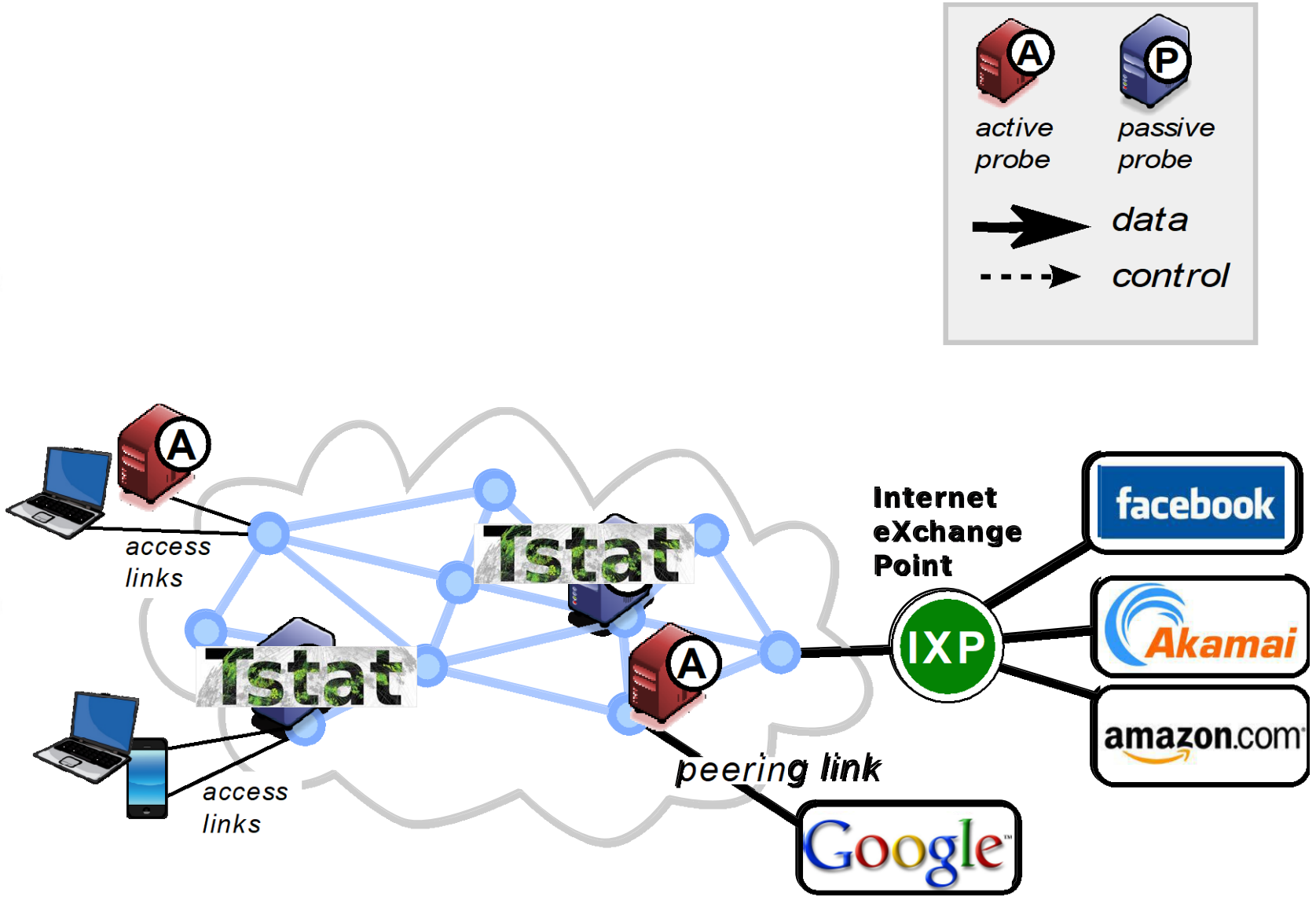
Monitoring approach



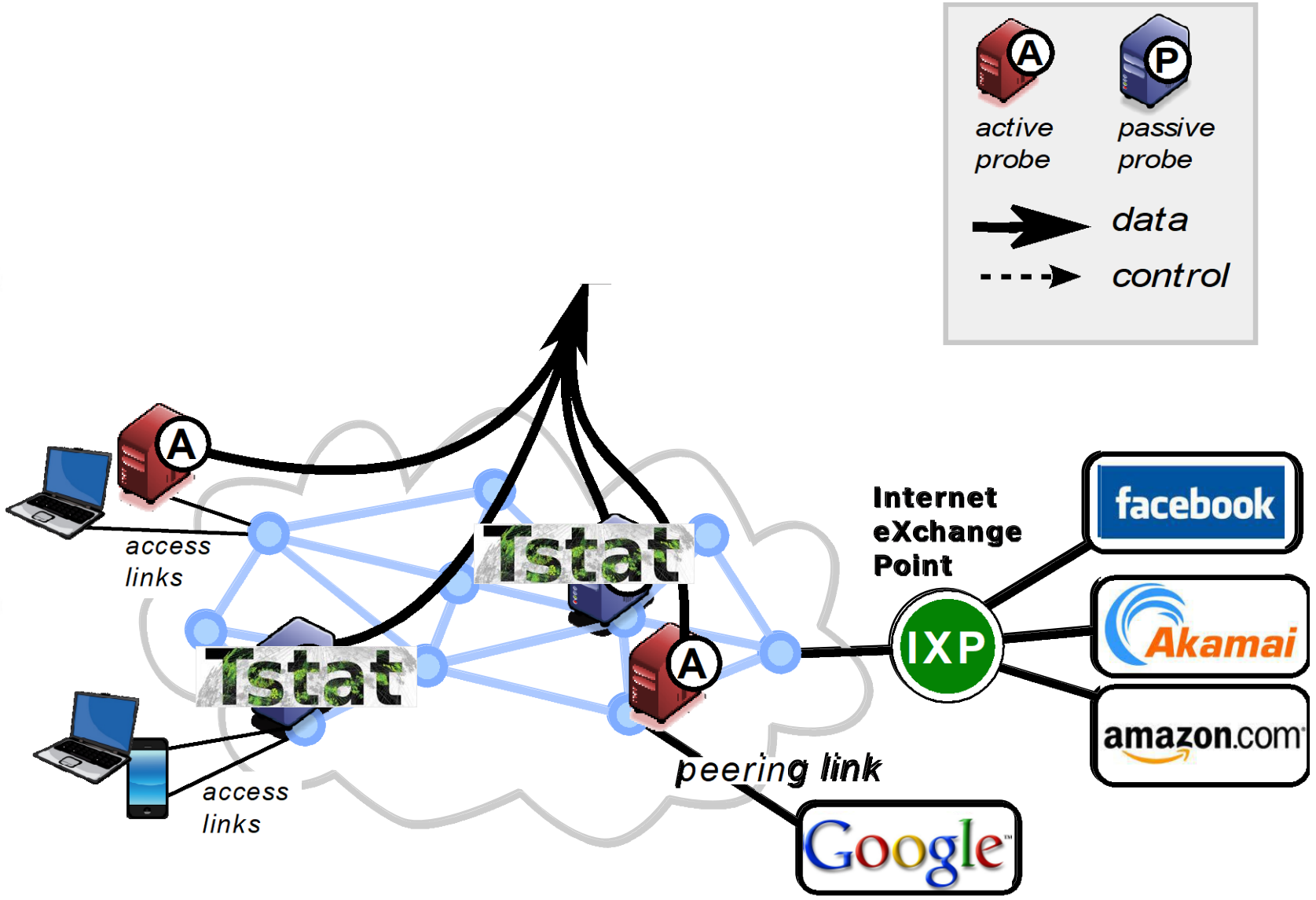
Monitoring approach



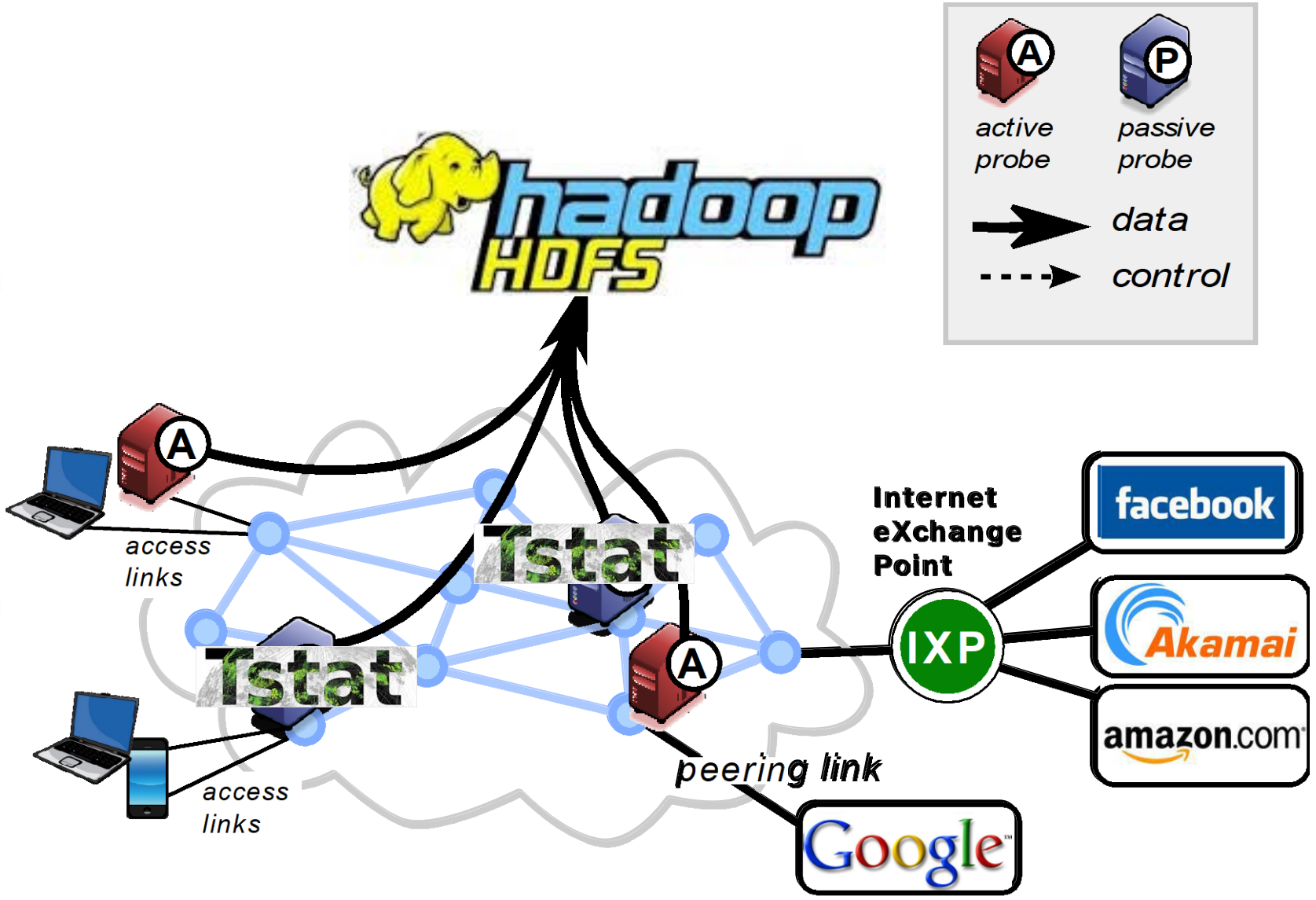
Monitoring approach



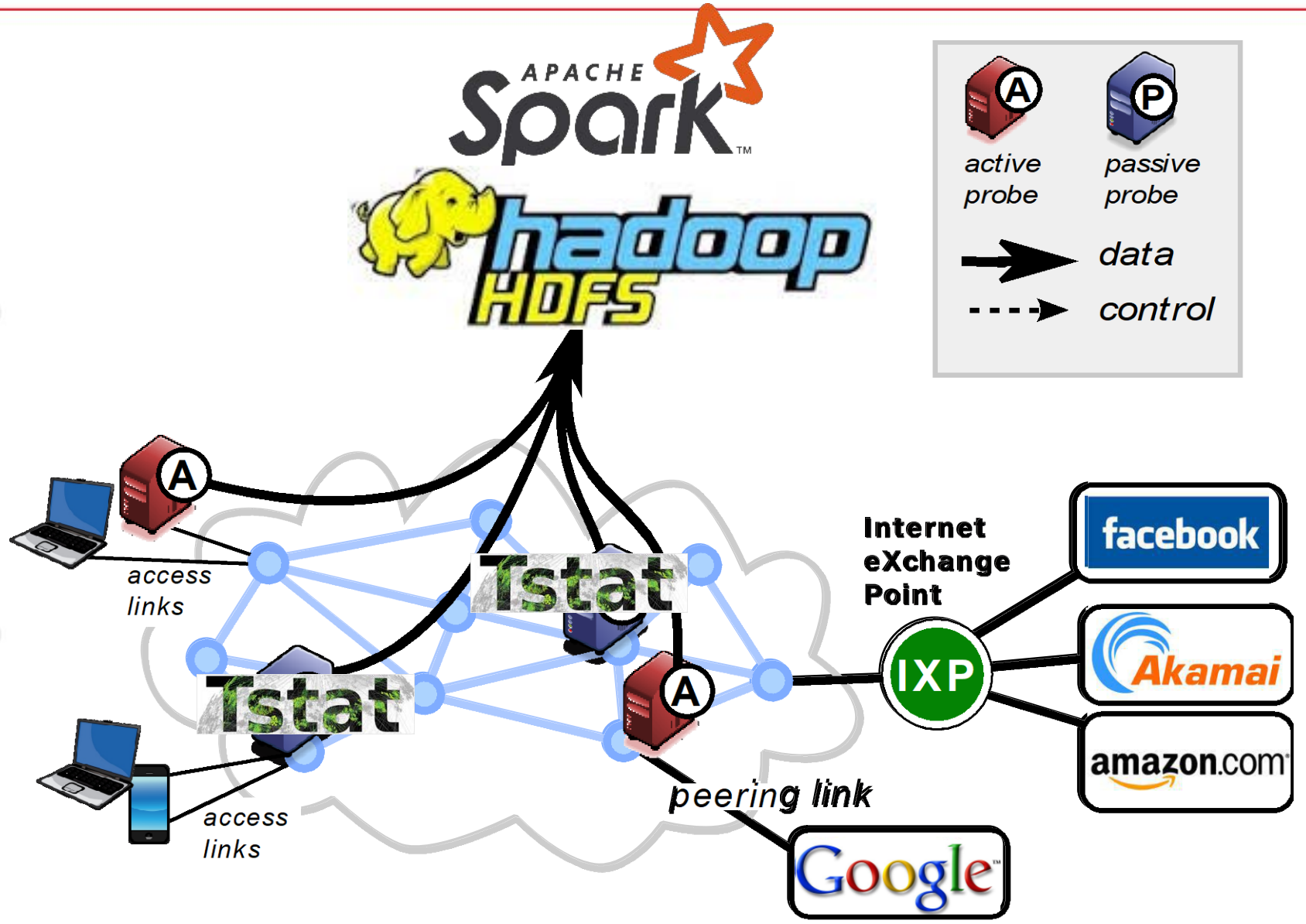
Monitoring approach



Monitoring approach

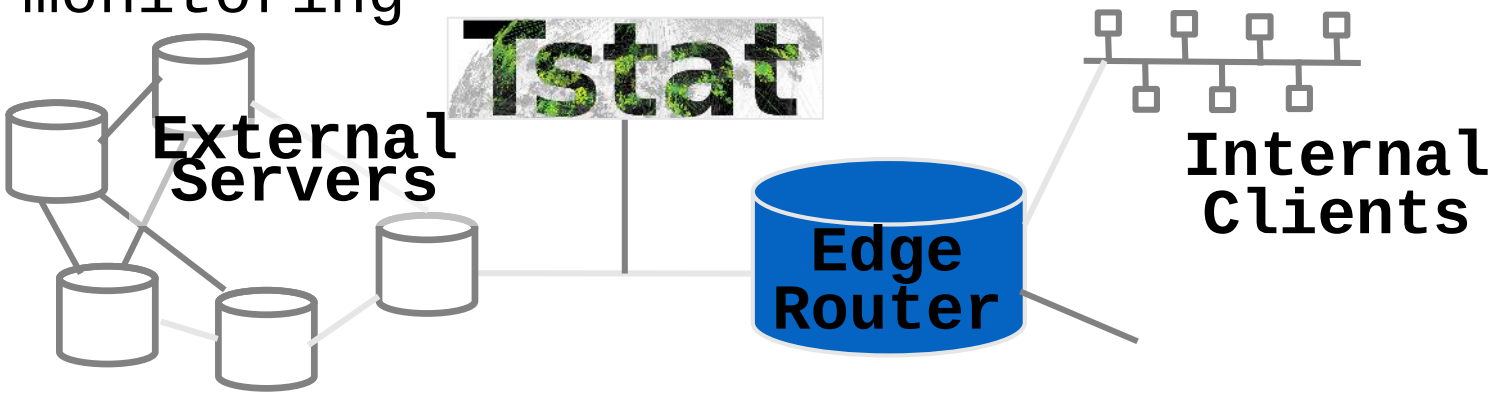


Monitoring approach



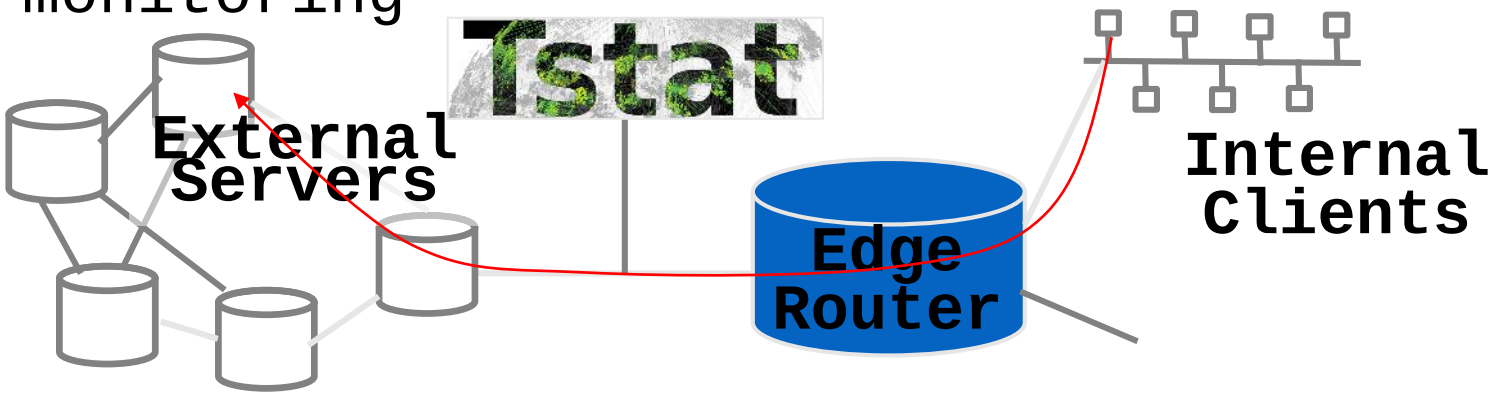
Tstat: Polito passive probe

- Statistical Analysis at IP/UDP/TCP
  - Passive inspection of packet headers
  - Rebuild bidirectional flow connections
  - Features real-time analysis (pcap, DAG, DPDK)
  - Offers persistent and scalable monitoring



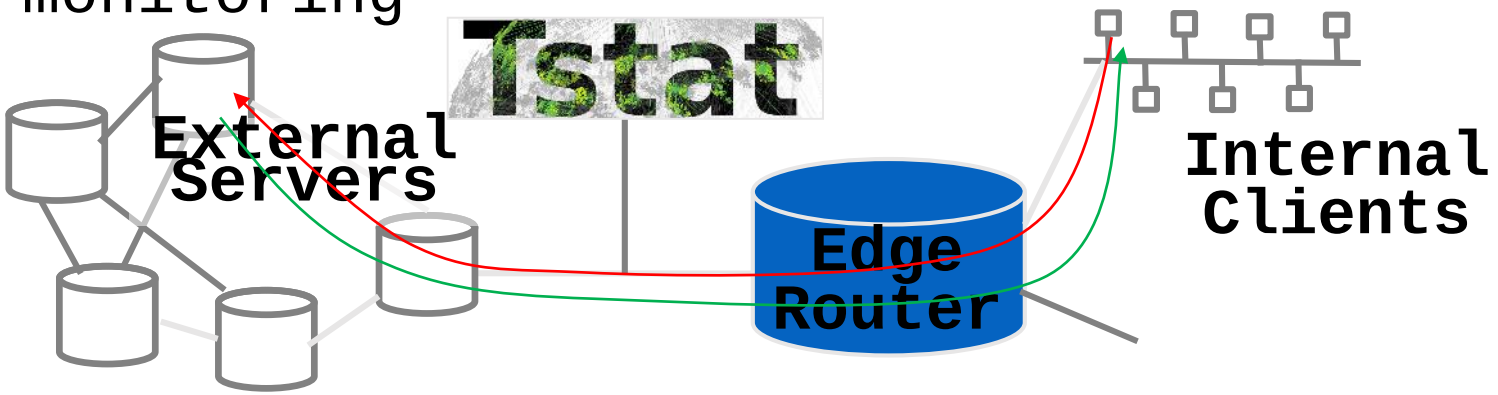
Tstat: Polito passive probe

- Statistical Analysis at IP/UDP/TCP
  - Passive inspection of packet headers
  - Rebuild bidirectional flow connections
  - Features real-time analysis (pcap, DAG, DPDK)
  - Offers persistent and scalable monitoring



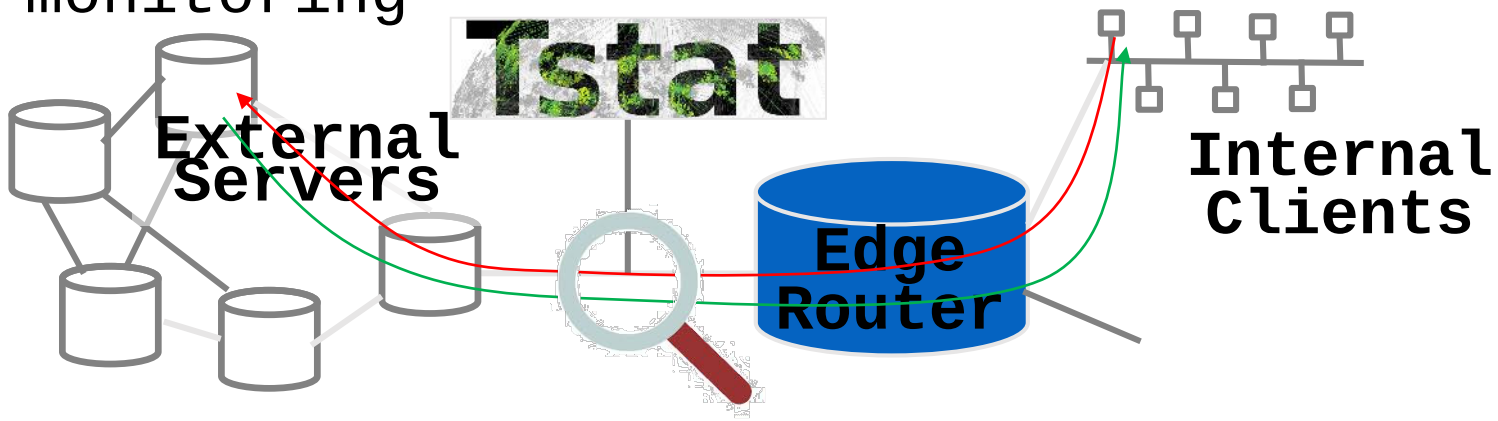
Tstat: Polito passive probe

- Statistical Analysis at IP/UDP/TCP
  - Passive inspection of packet headers
  - Rebuild bidirectional flow connections
  - Features real-time analysis (pcap, DAG, DPDK)
  - Offers persistent and scalable monitoring



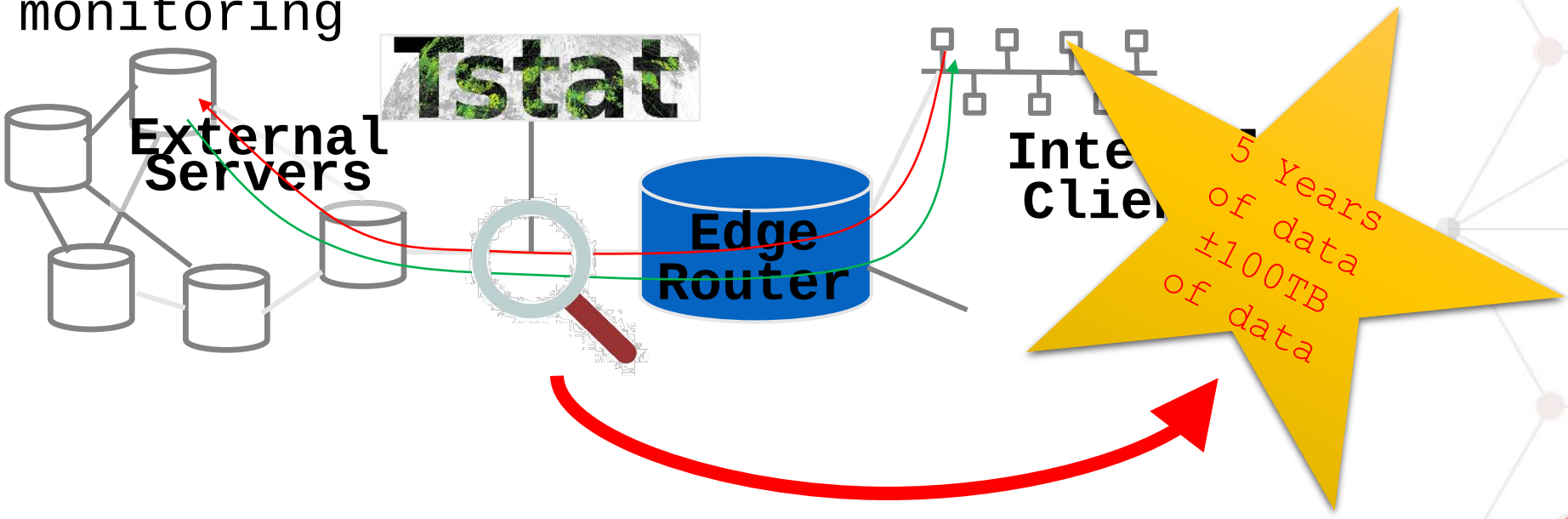
Tstat: Polito passive probe

- Statistical Analysis at IP/UDP/TCP
  - Passive inspection of packet headers
  - Rebuild bidirectional flow connections
  - Features real-time analysis (pcap, DAG, DPDK)
  - Offers persistent and scalable monitoring

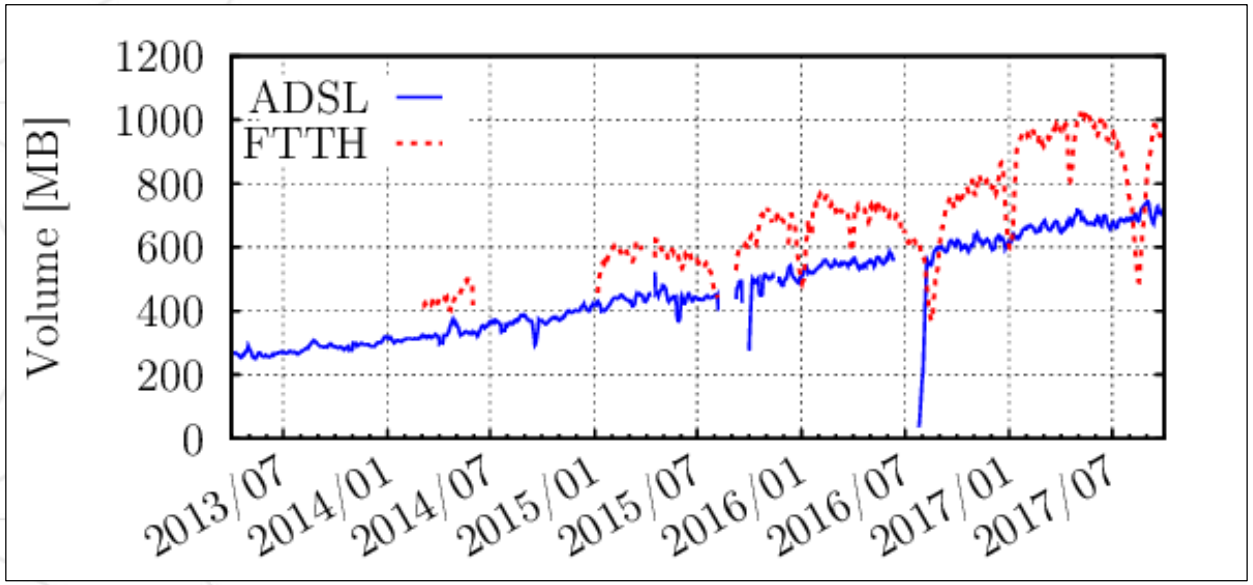


Tstat: Polito passive probe

- Statistical Analysis at IP/UDP/TCP
  - Passive inspection of packet headers
  - Rebuild bidirectional flow connections
  - Features real-time analysis (pcap, DAG, DPDK)
  - Offers persistent and scalable monitoring



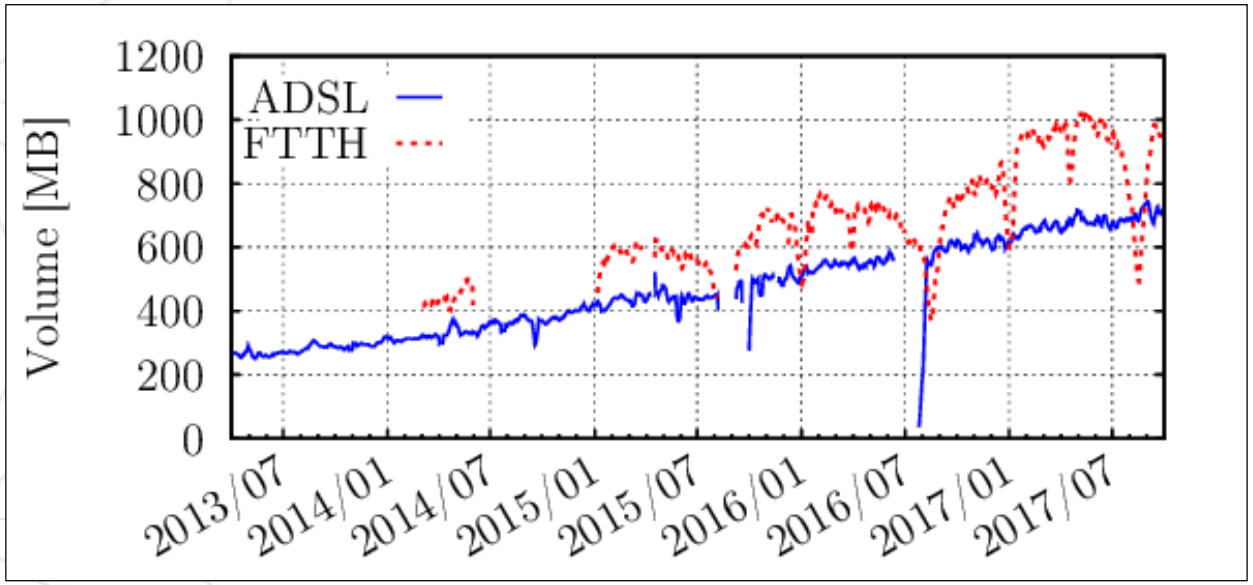
The Internet over the years

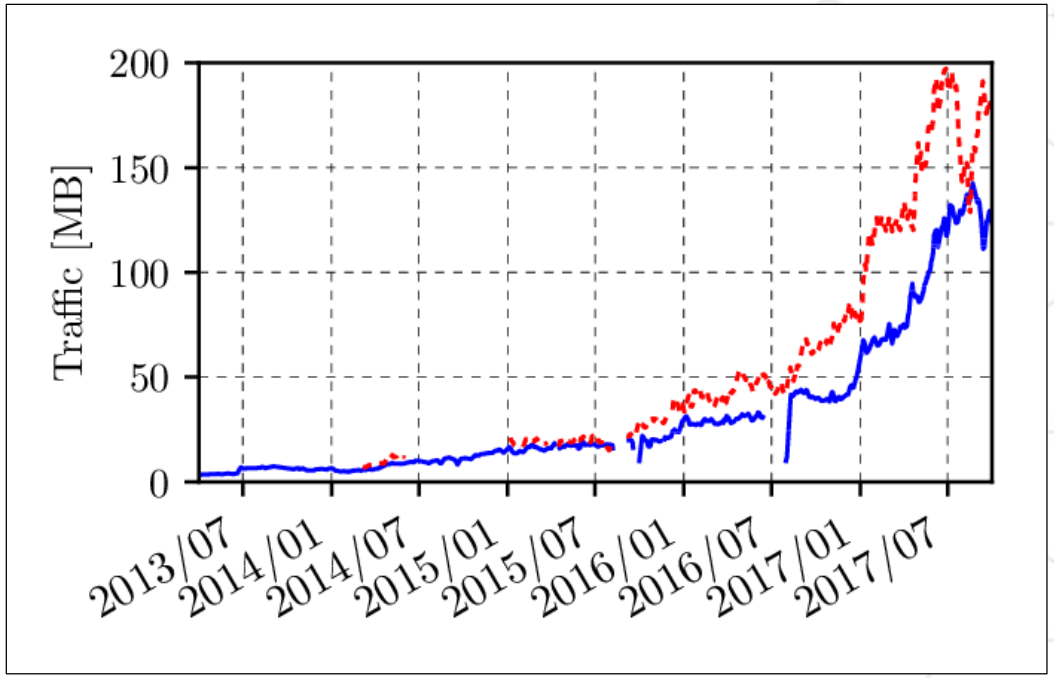


"Cost" of a broadband subscriber per day

Trevisan, M.; Giordano, D.; Drago, I.; Mellia, M.; Munafo', M., *Five years at the edge*, in: ACM CoNEXT 2018

The Internet over the years



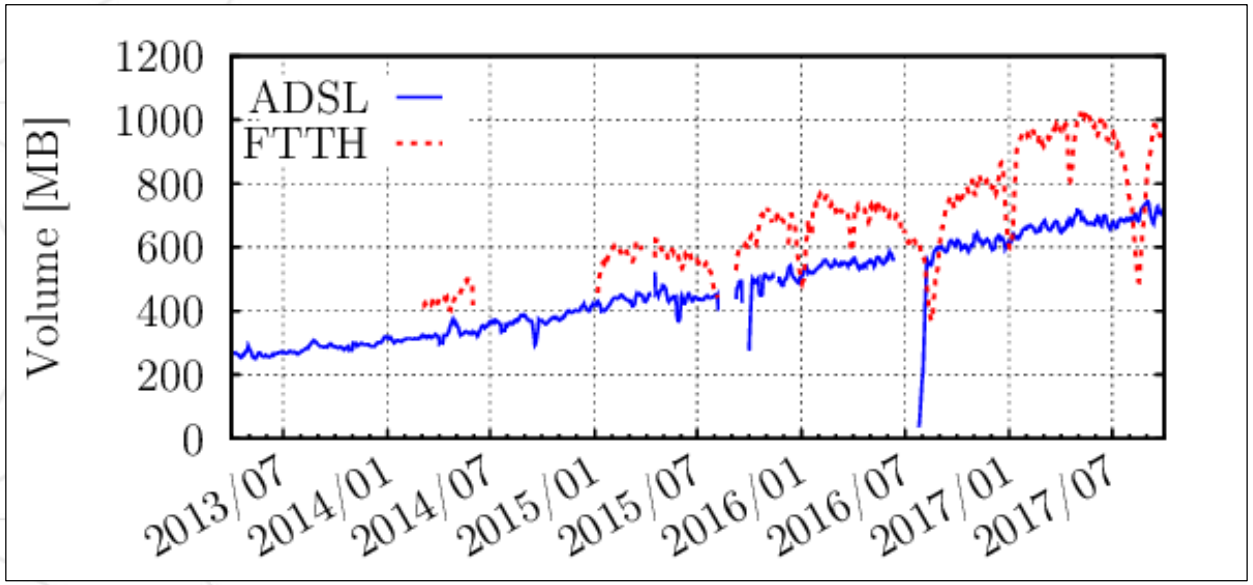


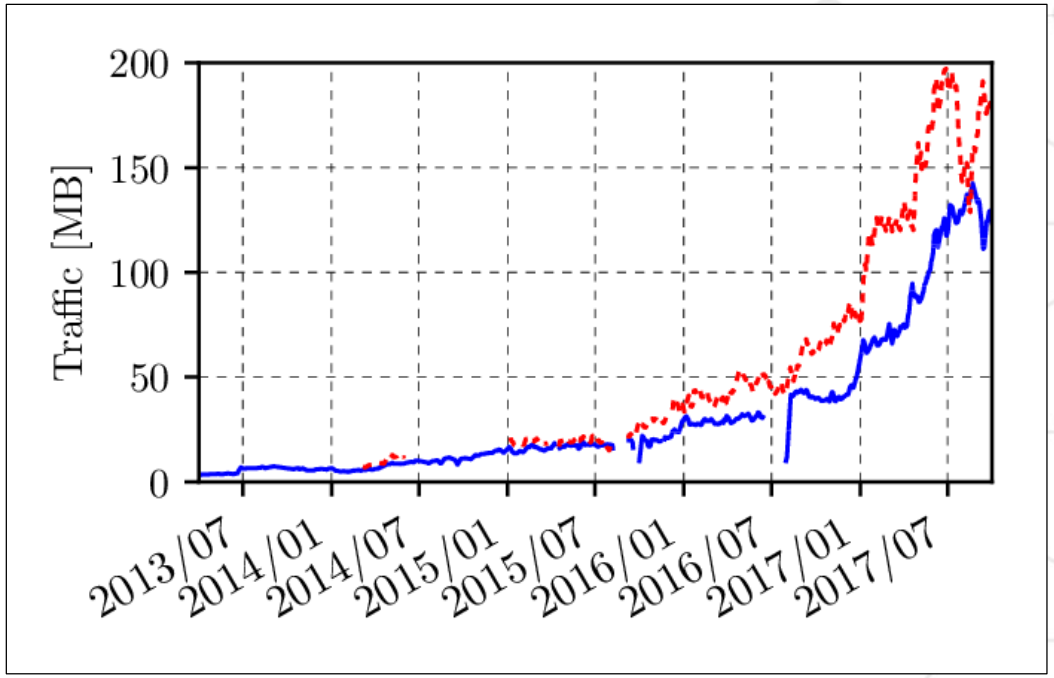
"Cost" of a broadband subscriber per day

Instagram: New elephant in the net [MB/subscriber/day]

Trevisan, M.; Giordano, D.; Drago, I.; Mellia, M.; Munafo', M., *Five years at the edge*, in: ACM CoNEXT 2018

The Internet over the years





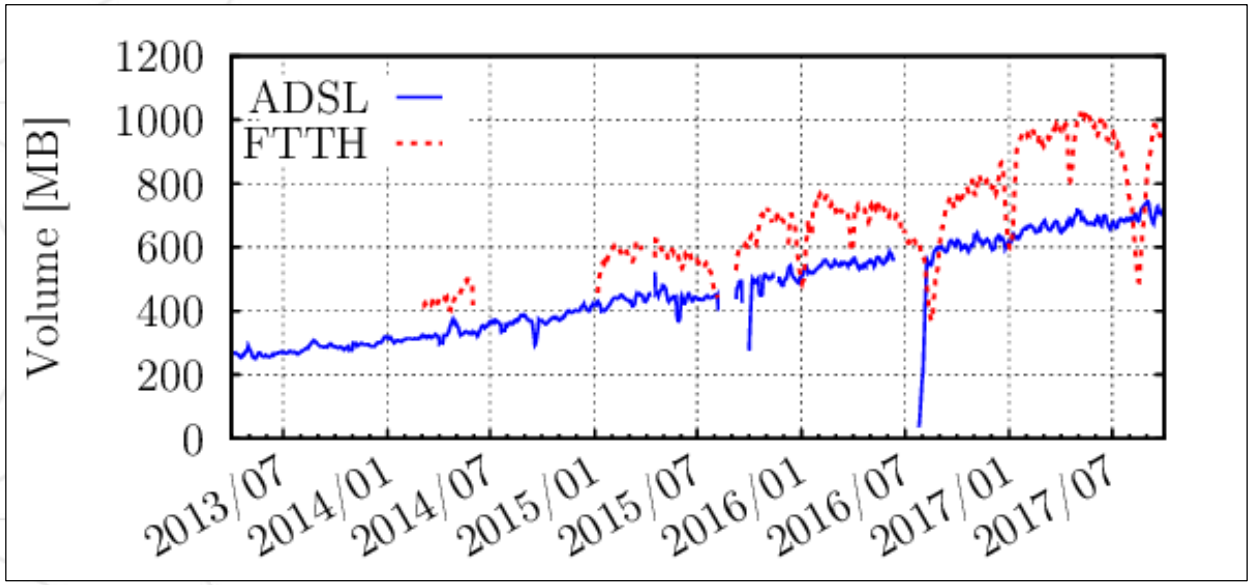
"Cost" of a broadband subscriber per day

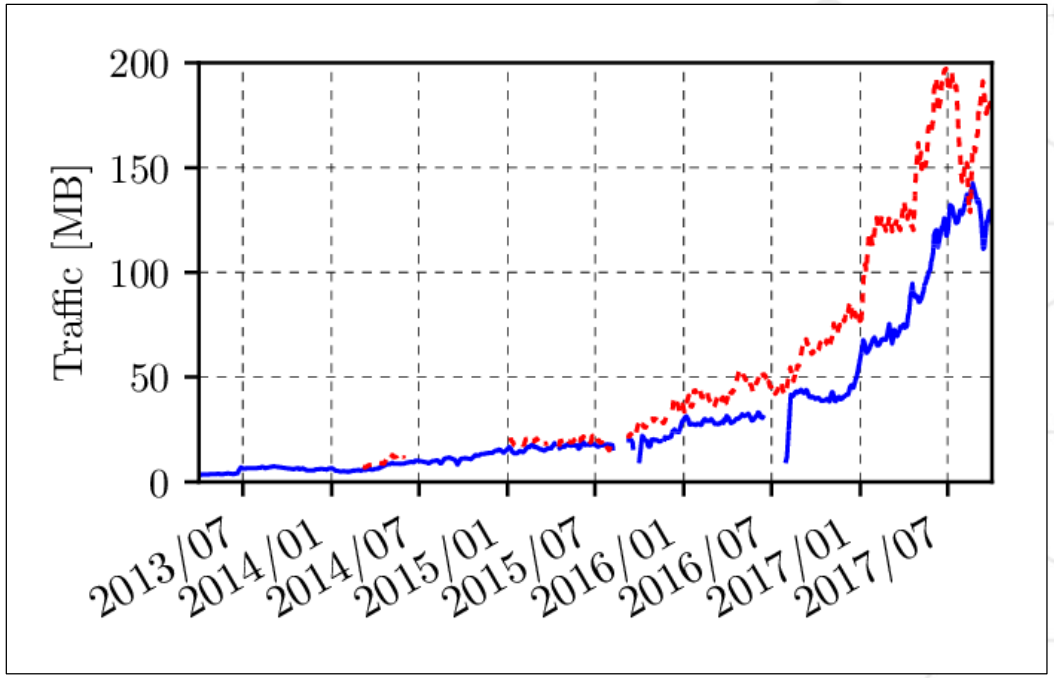
Instagram: New elephant in the net [MB/subscriber/day]

- These are benign services, which do not try to evade the monitoring

Trevisan, M.; Giordano, D.; Drago, I.; Mellia, M.; Munafo', M., *Five years at the edge*, in: ACM CoNEXT 2018

The Internet over the years





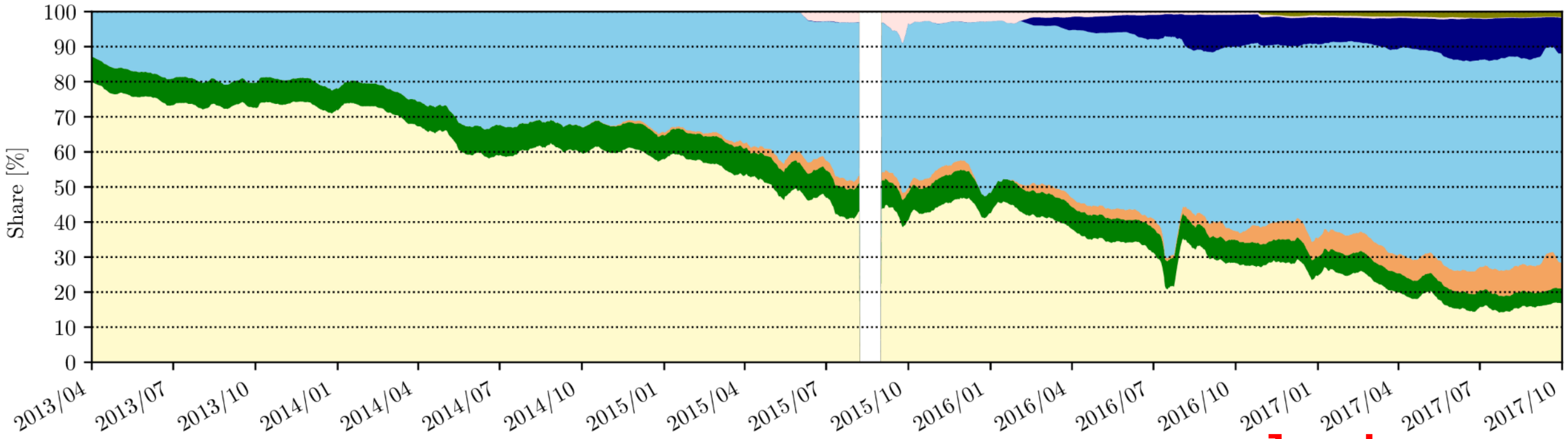
"Cost" of a broadband subscriber per day

Instagram: New elephant in the net [MB/subscriber/day]

- These are benign services, which do not try to evade the monitoring
- Algos to identify traffic even when encryption is in place

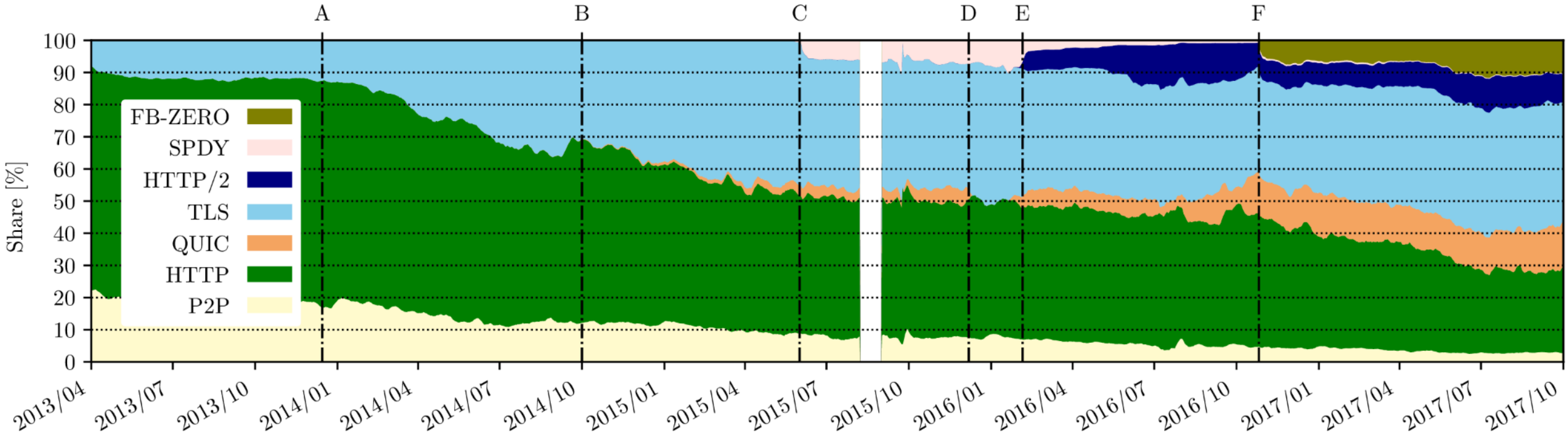
Trevisan, M.; Giordano, D.; Drago, I.; Mellia, M.; Munafo', M., *Five years at the edge*, in: ACM CoNEXT 2018

Protocol usage over the years



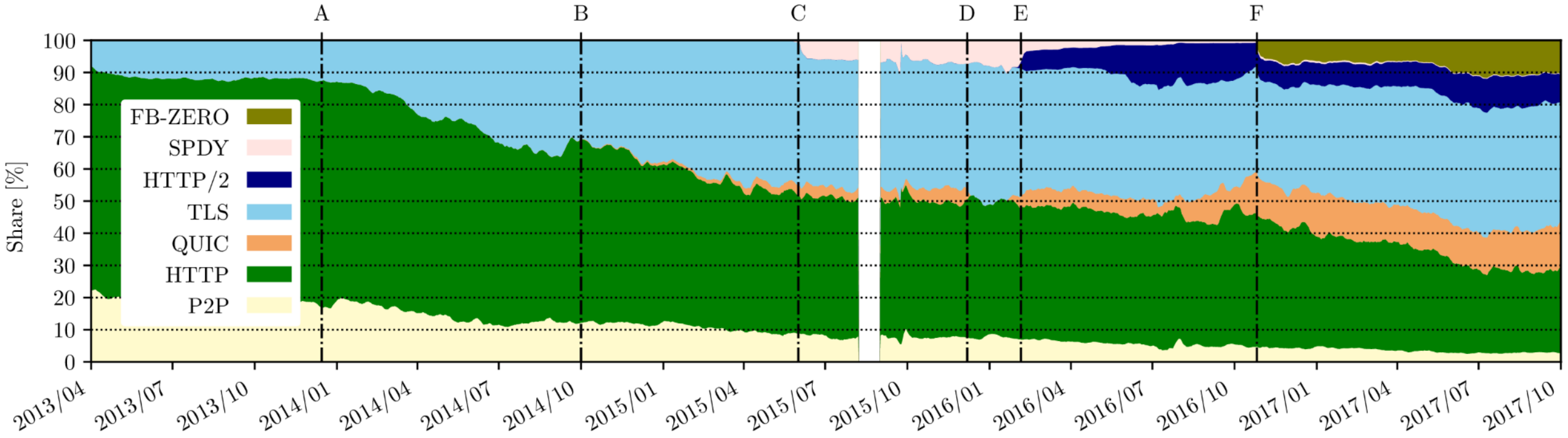
upload

Protocol usage over the years



download

Protocol usage over the years



download

- These figures miss what is actual users' traffic and what is unsolicited/background/malicious traffic

Unanswered incoming traffic

Unanswered incoming traffic

- **Low volume, high numbers of flows**
- E.g., failed “TCP handshakes”

Unanswered incoming traffic

- **Low volume, high numbers of flows**
- E.g., failed “TCP handshakes”
- **Contributing these logs to the community is very hard**
  - Even for traffic in our university network
  - Even anonymized
  - Users’ routine on-line/off-line
  - Scanning if host is active

Unanswered incoming traffic

- **Low volume, high numbers of flows**
- E.g., failed “TCP handshakes”
- **Contributing these logs to the community is very hard**
  - Even for traffic in our university network
  - Even anonymized
  - Users’ routine on-line/off-line
  - Scanning if host is active
- Yet letting people perform analysis in our premises is generally fine

~~Darknets @Polito~~

Internet Telescope @Polito

POLITECNICO

Google Internet telescopes

All Shopping Images News Videos More Settings Tools Collections SafeSearch

slooh android worldwide india long astronomy distance affordable medium sized rough beginner high tech personal space unusual modern day 30 cm human as

Sponsored

$1,299.95
Celestron NexStar 8SE Telescope...
High Point Scientific

$1,699.00
USED CELESTRON CPC925 TELESCOP...
OPT Telescopes

$18,999.00
Meade 16 LX600 ACF Telescope with...
High Point Scientific

$299.99
Orion AstroView 90mm Equatorial...
Orion Telescopes & ...
★★★★½ (44)

$499.00
Meade StarNavigator Next Generation...
OPT Telescopes
★★★½☆ (16)

View all

Internet in the promotion ...
virtualtelescope.eu

iTelescope.Net
itelescope.net

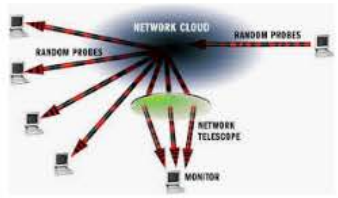
Robotic Telescopes for Educational Outreach
insightobservatory.com

Robotic Telescopes for Ed...
insightobservatory.com

Online Telescopes - Uni...
universetoday.com

Internet Telescope - View ...
indiamart.com

SPIRIT: An eye on the skies of Perth ...
perthcactus.com



The UCSD Network Telescope
caida.org

POLITECNICO

Google Internet telescopes

All Shopping Images News Videos More Settings Tools Collections SafeSearch

slooh android worldwide india long astronomy distance affordable medium sized rough beginner high tech personal space unusual modern day 30 cm human as

Sponsored

$1,299.95
Celestron NexStar 8SE Telescope...
High Point Scientific

$1,699.00
USED CELESTRON CPC925 TELESCOP...
OPT Telescopes

$18,999.00
Meade 16 LX600 ACF Telescope with...
High Point Scientific

$299.99
Orion AstroView 90mm Equatorial...
Orion Telescopes & ...
★★★★½ (44)

$499.00
Meade StarNavigator Next Generation...
OPT Telescopes
★★★½☆ (16)

View all

Internet in the promotion ...
virtualtelescope.eu

iTelescope.Net
itelescope.net

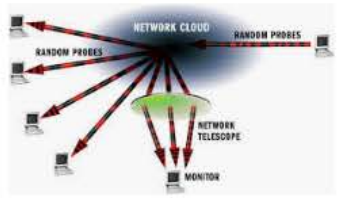
Robotic Telescopes for Educational Outreach
insightobservatory.com

Robotic Telescopes for Ed...
insightobservatory.com

Online Telescopes - Uni...
universetoday.com

Internet Telescope - View ...
indiamart.com

SPIRIT: An eye on the skies of Perth ...
perthcactus.com



The UCSD Network Telescope
caida.org

Google

Internet telescopes

All | Shopping | Images | News | Videos | More | Settings | Tools | Collections | SafeSearch

slooh | android | worldwide | india | long | astronomy | distance | affordable | medium sized | rough | beginner | high tech | personal | space | unusual | modern day | 30 cm | human

Sponsored

$1,299.95
Celestron NexStar 8SE Telescope...
High Point Scientific

$1,699.00
USED CELESTRON CPC925 TELESCOP...
OPT Telescopes

$18,999.00
Meade 16 LX600 ACF Telescope with...
High Point Scientific

$299.99
Orion AstroView 90mm Equatorial...
Orion Telescopes & ...
★★★★½ (44)

$499.00
Meade StarNavigator Next Generation...
OPT Telescopes
★★★½☆ (16)

View all

Internet in the promotion ...
virtualtelescope.eu

iTelescope.Net
itelescope.net

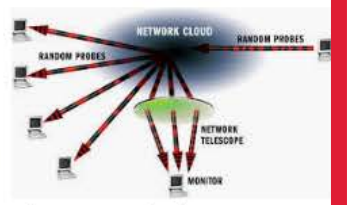
Robotic Telescopes for Educational Outreach
insightobservatory.com

Robotic Telescopes for Ed...
insightobservatory.com

Online Telescopes - Uni...
universetoday.com

Internet Telescope - View ...
indiamart.com

SPIRIT: An eye on the skies of Perth ...
perthcactus.com



The UCSD Network Telescope
caida.org

Why?

Why?

- From ISPs (and our IT) we get questions such:
  - What is this weird activity on port X ?
  - Are there hosts in my network joining botnet Z ?
  - Anyone vulnerable to Y ?
  - Latest one: Is my network sending traffic to darknets? Which nodes?
  - ...

Why?

- From ISPs (and our IT) we get questions such:
  - What is this weird activity on port X ?
  - Are there hosts in my network joining botnet Z ?
  - Anyone vulnerable to Y ?
  - Latest one: Is my network sending traffic to darknets? Which nodes?
  - ...
- With passive TSTAT traces we perform post-mortem analysis
  - Often too little information for stealth cases (not the big scans)

Why?

- From ISPs (and our IT) we get questions such:
  - What is this weird activity on port X ?
  - Are there hosts in my network joining botnet Z ?
  - Anyone vulnerable to Y ?
  - Latest one: Is my network sending traffic to darknets? Which nodes?
  - ...
- With passive TSTAT traces we perform post-mortem analysis
  - Often too little information for stealth cases (not the big scans)
- **Darknets and Honeypots**
  - Get context on unsolicited traffic we see in production
  - Transfer knowledge from our lab to other networks (!?)

Data sources

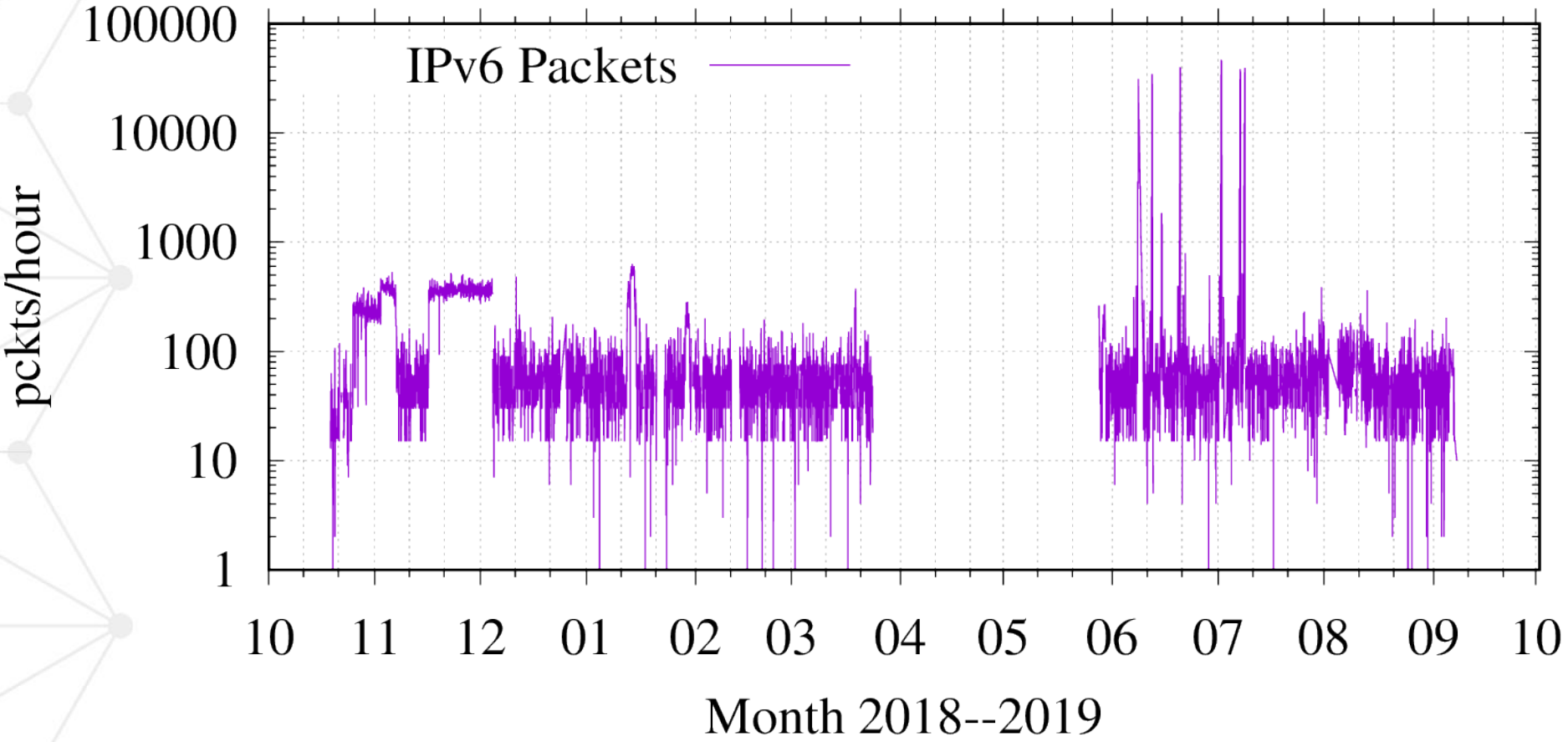
Data sources

- Internet darknet @Polito
  - GaRR Autonomous System
  - Few IP addresses – **now 3 x /24 IPv4 (to be expanded in GaRR)**
  - Long-term: any unused IP addresses @polito (even temporarily)
  - **IP addresses recently used in production**

Data sources

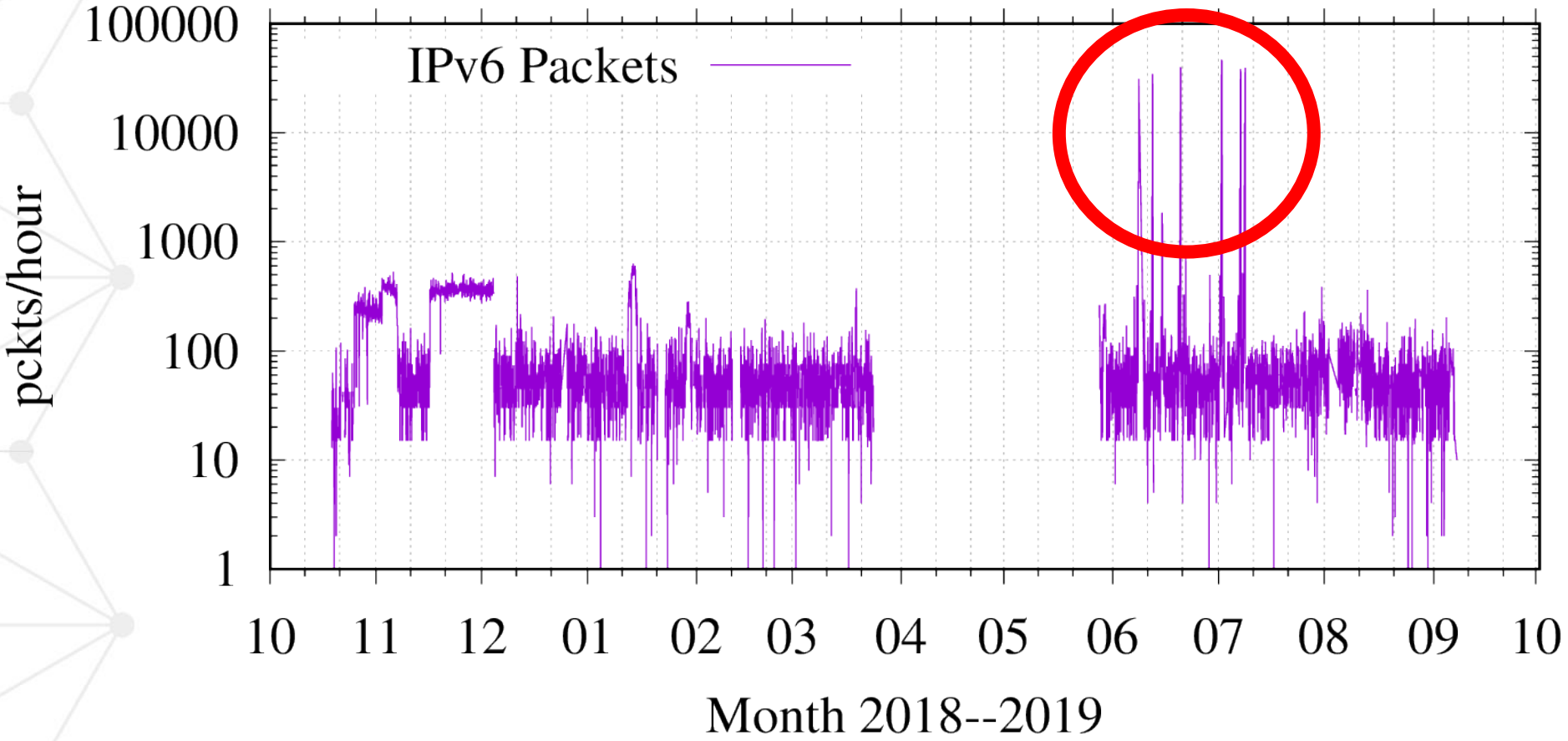
- Internet darknet @Polito
  - GaRR Autonomous System
  - Few IP addresses – **now 3 x /24 IPv4 (to be expanded in GaRR)**
  - Long-term: any unused IP addresses @polito (even temporarily)
  - **IP addresses recently used in production**
- Internet darknet @RNP (BR)
  - **/19 IPv4**
  - **/33 + /48 IPv6**
  - **IPv4** allocated to production traffic few years ago

IPv6 (baseline)



- Dominated by researchers (mostly ICMPv6)
  - e.g., reverse lookup: yhu-ca.**caida**.ebox.ca, **caida-gw**.ip6.gtt.net
  - Big peaks: **researchscanner100.eecs.berkeley.edu** (sending TCP SYN packets)

IPv6 (baseline)



- Dominated by researchers (mostly ICMPv6)
  - e.g., reverse lookup: yhu-ca.**caida**.ebox.ca, **caida-gw**.ip6.gtt.net
  - Big peaks: **researchscanner100.eecs.berkeley.edu** (sending TCP SYN packets)

IPv4 sanity checks

The IPv4 darknets:

- **/15** in the Netherlands (baseline)
  (**30 GB of PCAPs/day**)
- **/19** in Brazil
  (**2.5 GB of PCAPs/day**)
- **3 /24** in Italy
  (**420 MB of PCAPs/day**)
- when comparing darknets, extract **samples of similar size (# IP addresses)**

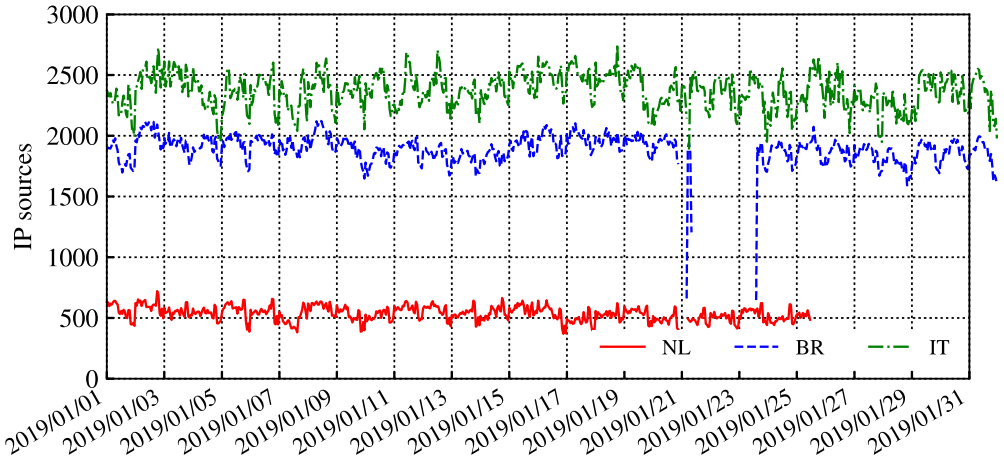
Methodology

- Get data from a large and more established darknet (@SurfNet)
- Compare traffic among the darknets
- Check if differences are inline with the literature
  - CAIDA/Merit‘s data [*]

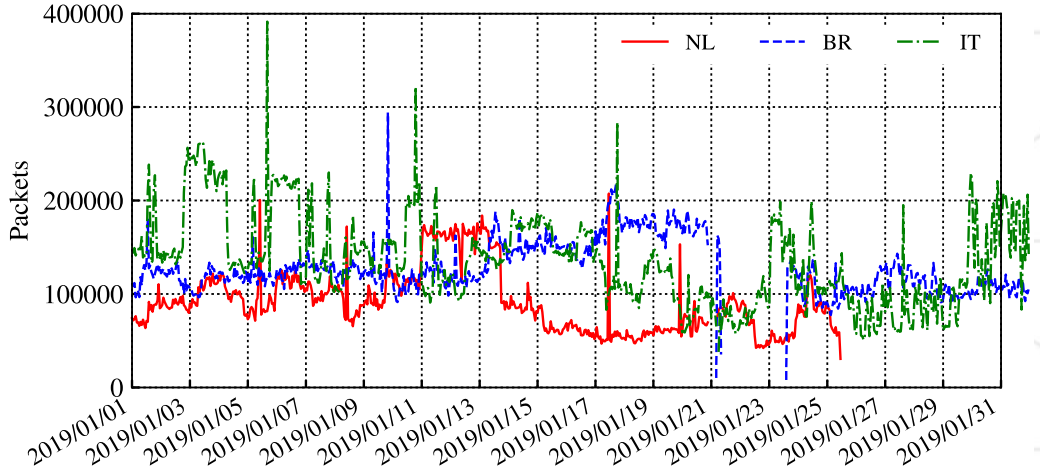
[*] K. Benson, A. Dainotti, K. Claffy, A. C. Snoeren, and M. Kallitsis, “Leveraging Internet Background Radiation for Opportunistic Network Analysis,” in Proc. of the IMC, 2015, pp. 423-436.

Temporal patterns

Top-talkers (at least 10 flows in 1-hour bin)



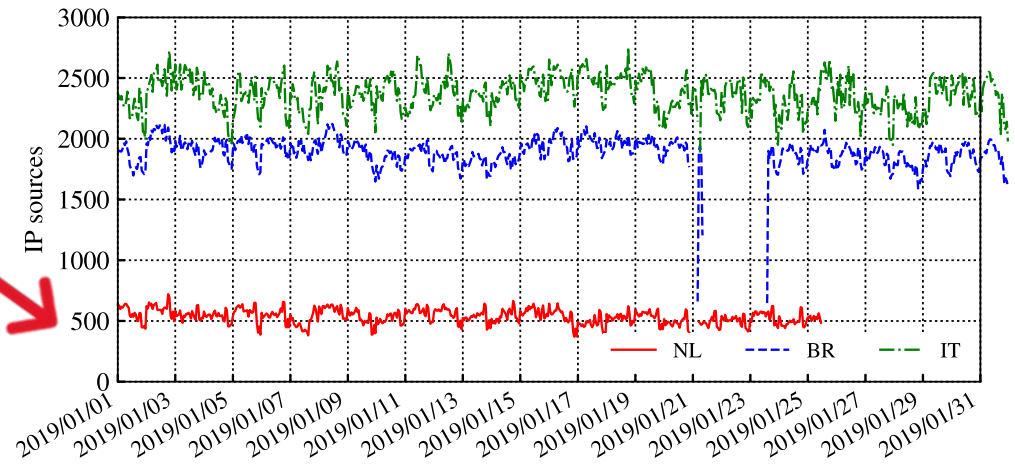
Number of distinct source IPs

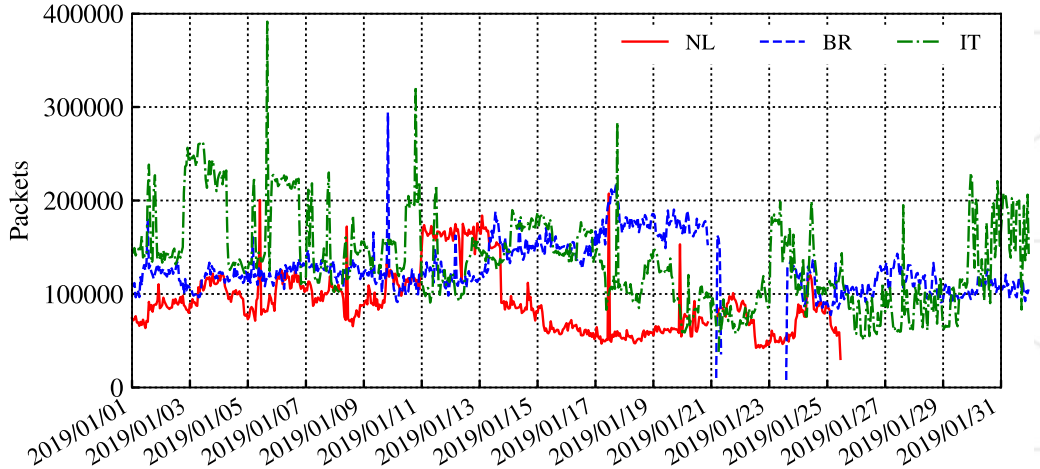


Number of packets

Temporal patterns

Top-talkers (at least 10 flows in 1-hour bin)





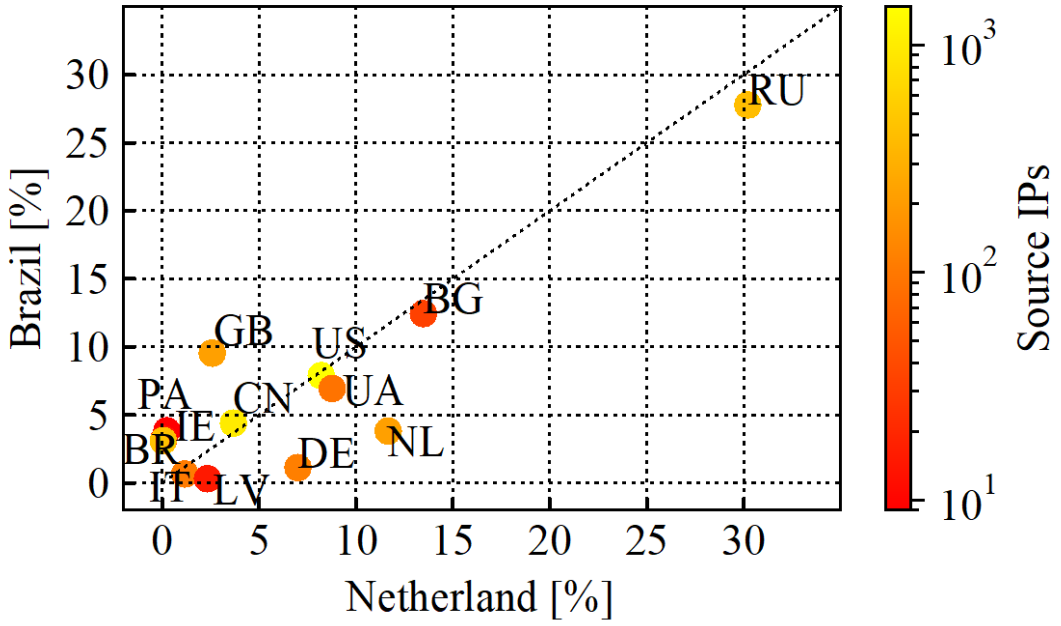
Number of distinct source IPs

Number of packets

#packets is **noisy and irregular**, and differs for darknets.
IP address of senders show a **more regular** distribution over time

Sources – countries

Top-talkers (at least 10 flows in 1-hour bin)



Packets from almost **all countries** are seen in **all** darknets

The **most active sources** are **similar**

Sources – ASes

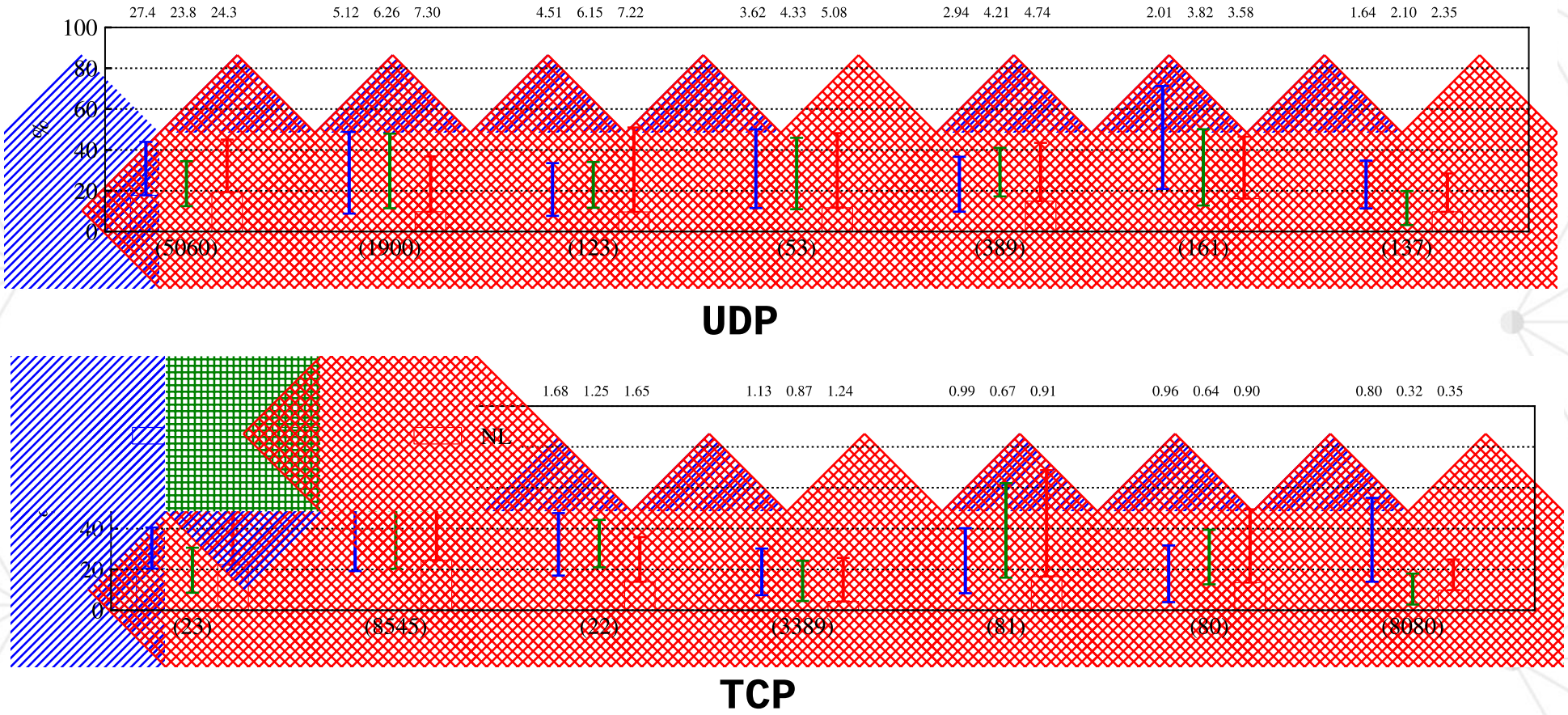
Top-talkers (at least 10 flows in 1-hour bin)

BR			NL			IT		
ASN	pkts (%)	IPs	ASN	pkts (%)	IPs	ASN	pkts (%)	IPs
49453	14.8	8	49505	10.57	15	43350	22.18	12
57043	10.72	15	**202325**	9.94	11	**204428**	7.17	24
202325	6.5	12	**204428**	7.52	20	**58271**	7.05	22
58271	5.18	19	**58271**	6.9	19	51852	6.69	5
204428	3.74	18	201912	5.8	8	**57043**	6.28	16

Very few IP addresses produce the largest amount of traffic

Most active ASes are visible in **all** darknets (mostly from **RU/CN/BG**)

Per-port breakdown

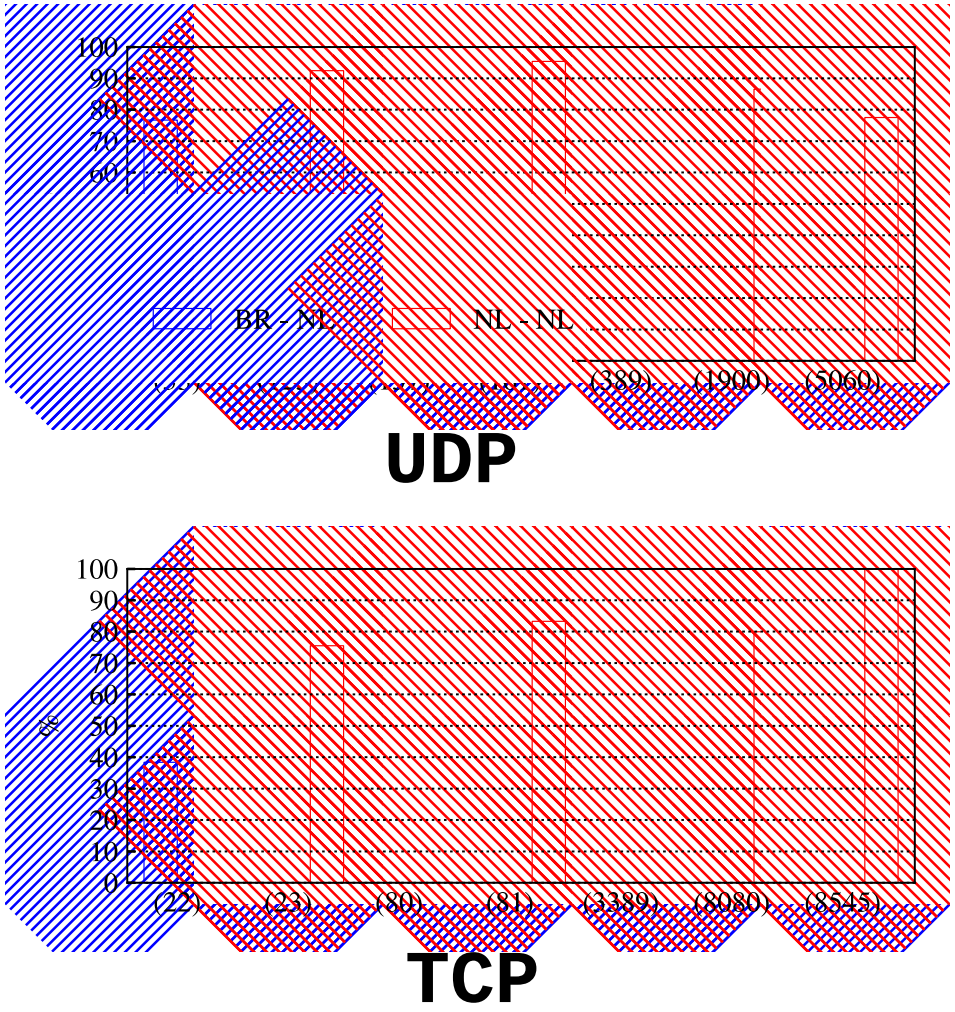


No big surprise either – the usual suspects are hit.

The most active IP produces the 10-20% of traffic

Per-port breakdown

How spread are the sources?

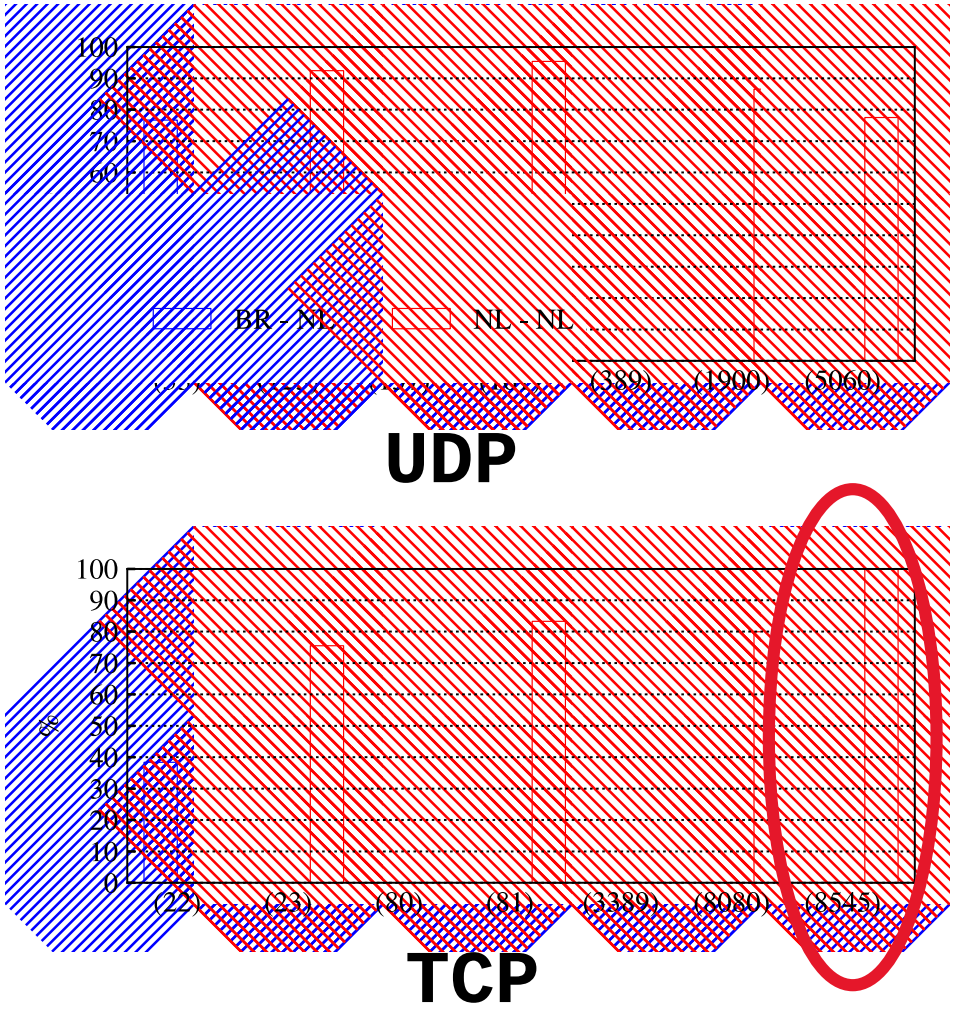


Jaccard Index to measure similarity between the traffic sources:

$$\frac{set(ASes_{BR}) \cap set(ASes_{NL})}{set(ASes_{BR}) \cup set(ASes_{NL})}$$

Per-port breakdown

How spread are the sources?



At least **half of the source ASes** are always visible on both darknets

TCP targets tend to be hit by **more distributed sources.**

Some exceptions

Summary

Summary

- Major properties follow those reported in literature
  - Destination ports are similar, packets coming from a significant number of ASes and almost all countries

Summary

- Major properties follow those reported in literature
  - Destination ports are similar, packets coming from a significant number of ASes and almost all countries
- Similar volume of packets (per darknet address) in the 3 deployments
  - Dominated by the heavy hitters, which are similar

Summary

- Major properties follow those reported in literature
  - Destination ports are similar, packets coming from a significant number of ASes and almost all countries
- Similar volume of packets (per darknet address) in the 3 deployments
  - Dominated by the heavy hitters, which are similar
- More diversity IP sources in the BR/IT darknets
  - IP addresses used in production more recently
  - Few packets sent by large number of sources (tail of popularity dist.)

Summary

- Major properties follow those reported in literature
  - Destination ports are similar, packets coming from a significant number of ASes and almost all countries
- Similar volume of packets (per darknet address) in the 3 deployments
  - Dominated by the heavy hitters, which are similar
- More diversity IP sources in the BR/IT darknets
  - IP addresses used in production more recently
  - Few packets sent by large number of sources (tail of popularity dist.)
- BR and IT darknet are operative since Sept 2018
- Data can be shared for research purposes

Beyond the darknets

Getting even more dust

- **HoneyPort**
  - Deploying flexible honeypots for adding context to darknet traces

- **Why:**
  - **We would like to add meta-data to traffic as much as we can, e.g.,**
    - **These packets are someone scanning with tool X**
    - **This is MIRAI botnet**
    - **... in production: these packets were a follow up of that scan**
  - **We are still in explorative phase, not clear how far we can go**

Goals and methodology

- Understand why someone is contacting us
  - Engage attackers
  - Produce fingerprints
  - Seed models to classify the packets

- Low-interaction honeypots (specific tasks)
  - **e.g., Save first packets after TCP/TLS handshake**
  - e.g., COWRIE, a ssh honeypot collecting binaries and passwords
  - ...

Goals and methodology

- Understand why someone is contacting us
  - Engage attackers
  - Produce fingerprints
  - Seed models to classify the packets

- Low-interaction honeypots (specific tasks)
  - **e.g., Save first packets after TCP/TLS handshake**
  - e.g., COWRIE, a ssh honeypot collecting binaries and passwords
  - ...
- High-interaction honeypots based on virtualization
  - Containers/VMs with realistic setup for high interaction
  - Build on top of **virtual machines** and **virtual networks**

Tones of honeypot options!

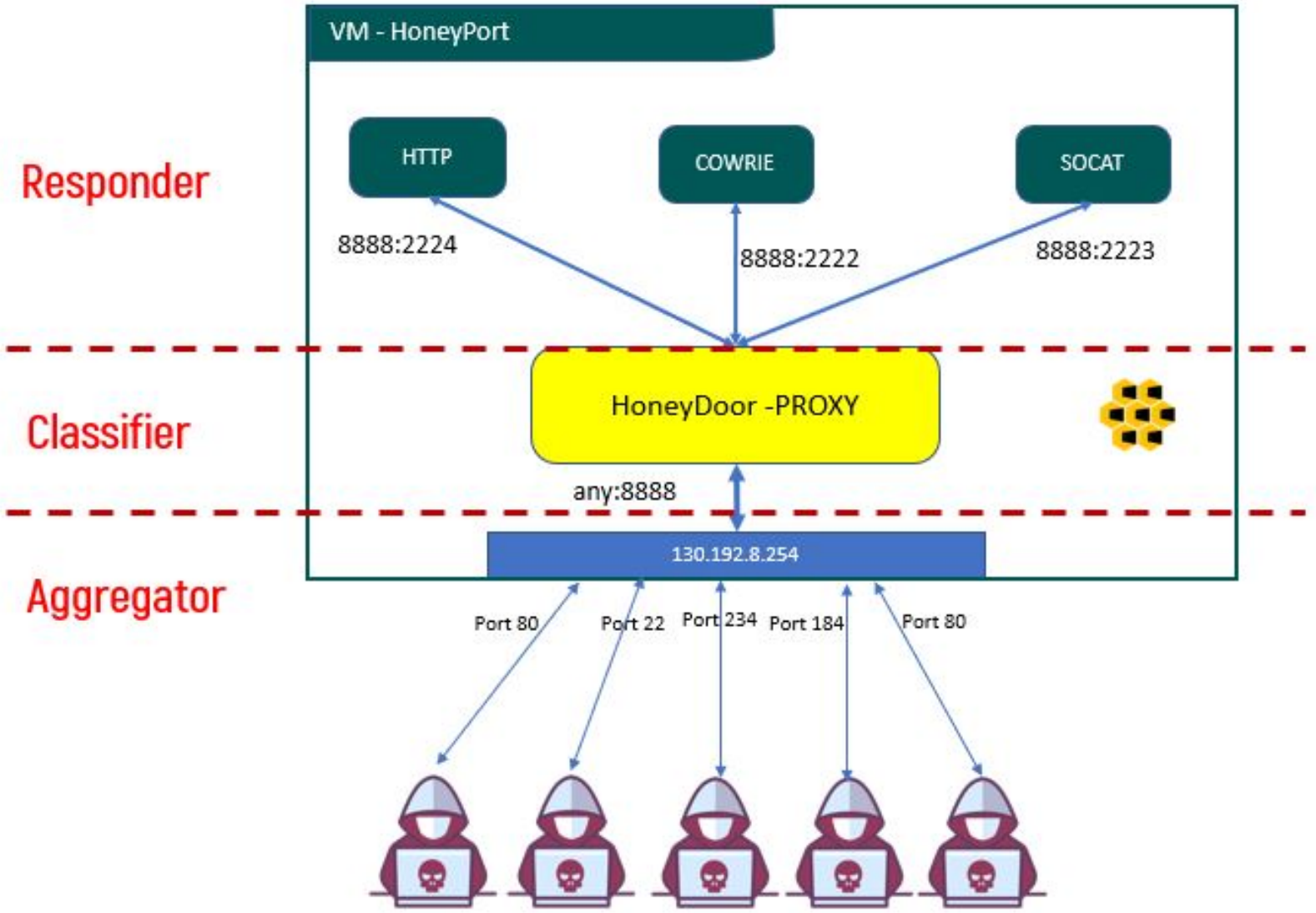
Tones of honeypot options!

Table III
CHRONOLOGICAL OVERVIEW AND CLASSIFICATION OF SERVER HONEYPOT SOFTWARE BY THEIR INTERACTION LEVEL TYPE. (+) INDICATES SOME ADDITIONAL SERVICES, (++) INDICATES MANY ADDITIONAL SERVICES, (*) MARKS VAGUE TIMESTAMPS.

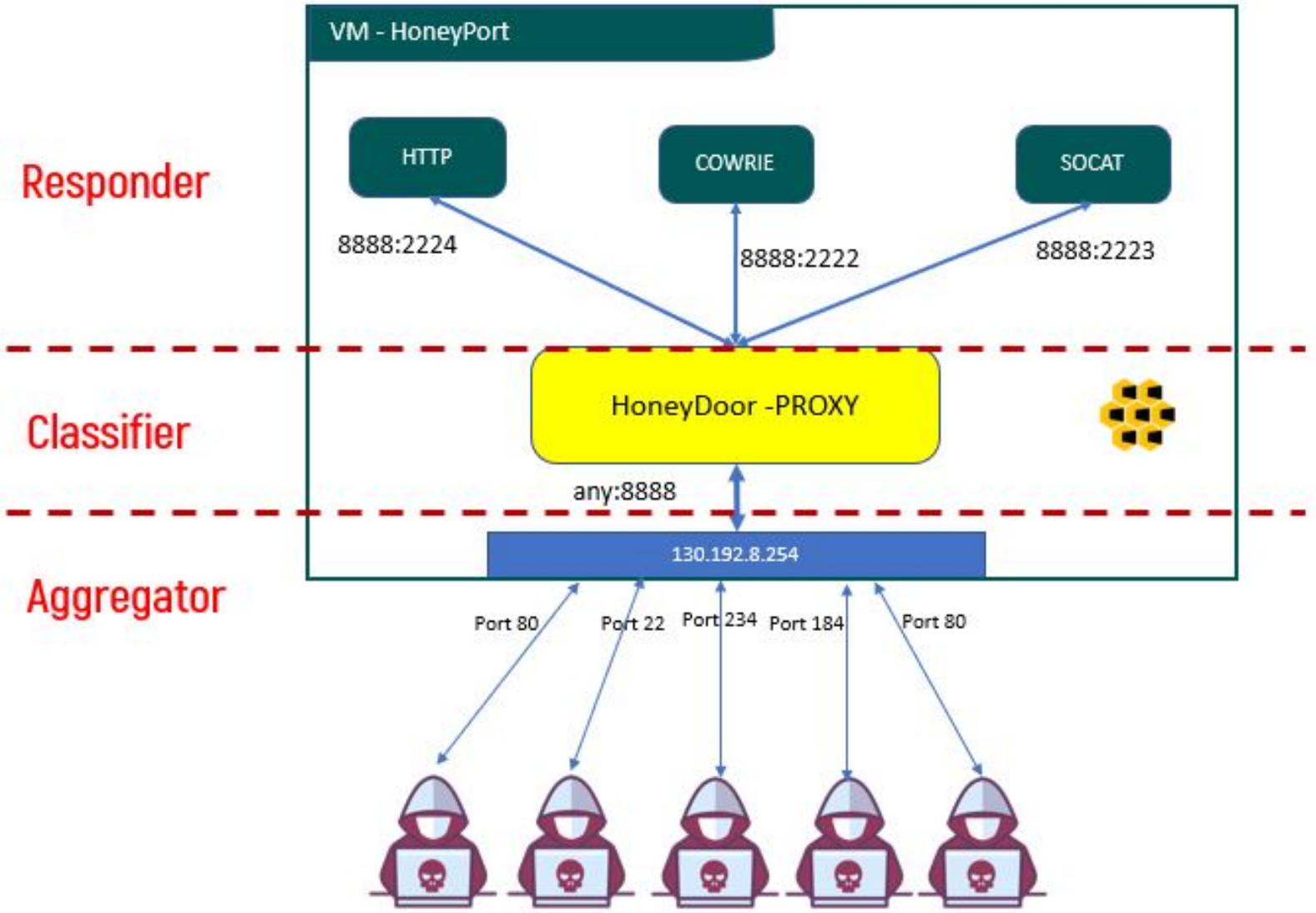
Type	Software	Maintenance: First	Maintenance: Last	Free	Focus: Services / Applications	Focus: Design / Details
low	DTK [31]	1997	1999	✓	SMB, SSH, DNS, FTP, Netstat(++)	implement many known vulnerabilities
low	BOF [32]	1998	1999	✓	Back Orifice, Telnet, SMTP(+)	waste intruders time, easy deployment
low	NetFacade [42]	1998	2002*	✗	*not specified*	class C network emulation
low	CyberCop Sting [33]	1999	1999	✗	Telnet, FTP, SendMail, SNMP	emulating different network devices
low	Specter [44]	1999	2005	✓	SMTP, FTP, HTTP and Telnet(+)	commercial deployment, decoy files
low	Sandtrap [97]	2002*	2002*	✗	dialup modem	war dialing trapping
low	single-honeypot [43]	2002	2002	✓	*all ports, but no emulation*	mere logging, KISS architecture
low	HoneyWeb [98]	2002	2003	✓	HTTP	various web server header emulation
low	LaBrea [39]	2002	2003	✓	*all ports, but no emulation*	simple TCP tarpit by SYN/ACK
low	SMTPot [38]	2002	2003	✓	SMTP	spam accumulation, KISS
low	THP [46]	2002	2003	✓	SSH (shell), HTTP, FTP	coexistence honeypot and real services
low	Jackpot [35]	2002	2004	✓	SMTP	delay spam, utilizing spam databases
low	FakeAP [79]	2002	2005	✓	802.11b AP beacons	p.o.c wireless honeypots
low	HoneyBot [34]	2002*	2007*	✓	SSH, SMTP, FTP, HTML(++)	windows vulnerabilities and GUI
low	BigEye [8]	2003	2003	✓	HTTP, FTP	emulation of different web servers
low	Spamhole [59]	2003	2003	✓	SMTP	silent dropping of emails
low	Spampot [90]	2003	2003	✓	SMTP	platform independence
low	HoneyPerl [36]	2003	2003	✓	HTTP, FTP, SMTP, Telnet(+)	extensibility by modules
low	Decoy Server [45]	2003*	2003	✗	SMTP, POP3	fake email server traffic
low	Smoke Detector [8]	2003*	2004*	✗	FTP, HTTP, IMAP, SSH, SMB(++)	honeypot as a hardware
low	NetBait [41]	2003	2007*	✗	*not specified*	honeypot as a service
low	HoneyD [28]	2003	2008	✓	HTTP, POP3, SMTP, FTP(+)	emulating heterogeneous networks
low	KFSensor [58]	2003	2015	✗	HTTP, SMTP, MSSQL, FTP(+)	commercial deployment of honeypots
low	SpamD [56]	2003	2015*	✓	SMTP	tarpit against spam
low	HOACD [15]	2004	2004	✓	*compare HoneyD*	live bootable CD (HoneyD, Arpd)
low	ProxyPot [57]	2004*	2004*	✓	SMTP	email spammer identification
low	Impost [37]	2004	2004	✓	*all ports, but no emulation*	full packet sniffing
low	Kojoney [63]	2005	2006	✓	SSH (shell activity)	first dedicated SSH honeypot
low	Mwcollect [53]	2005	2009	✓	*compare Nepenthes, Honeytrap*	merging Nepenthes and Honeytrap
low	Nepenthes [47]	2005	2009	✓	FTP, HTTP, TFTP, MSSQL(++)	capture worm payload
low	GHH [70]	2005	2013	✓	HHTP-Apache, PHP, MSSQL	crawler and search engines
low	Honeytrap [51]	2005	2015	✓	HTML, FTP(+), *dyn. emulation*	attacks via unknown protocols
low	HoneyPoint [96]	2006	2014	✗	*not specified*	ICS/Scada, back tracking intruders
low	Dionaea [49]	2009	2013	✓	SMB, FTP, SIP, MYSQL(++)	nepenthes successor, capture payload
low	Kippo [65]	2009	2014	✓	SSH (shell activity)	emulate entire shell interaction
low	Artemisa [78]	2010	2011	✓	VoIP, SIP	Bluetooth Malware
low	bluepot [81]	2010	2015	✓	Bluetooth	Bluetooth Malware
low	HoneySink [91]	2011	2011	✓	DNS, HTTP, FTP, IRC	bot sink holing
low	HoneyDroid [85]	2011	2014*	✓	*compare Kippo, HoneyTrap*	p.o.c Android OS honeypot
low	Glastopf [67]	2011	2015	✓	HTML, PHP, SQL	web applications, vulnerability types
low	Kojoney2 [64]	2012	2015	✓	SSH (shell activity)	applying Kojoneys lessons learned
low	Conpots [99]	2013	2015	✓	kamstrup, BACnet, modbus	ICS and SCADA architectures
low	IoTPOT [85]	2014*	2015	✓	telnet	IoT (ARM, MIPS, and PPC)
low	honeypot-camera [86]	2014	2015	✓	HTTP	Tornado Web, Webcam Server
low	Shockpot [87]	2014	2015	✓	Apache, Bash	Shellshock vulnerability
low	Cowrie [66]	2014	2015	✓	SSH (shell activity)	Kippos successor
low	Canarytokens [99]	2015	2016	✓	URLs, bitcoin, PDF	honeypot tokens
low	elastichoney [69]	2015	2015	✓	elasticsearch	elasticsearch RCEs
high	Sebek [97]	2003	2011	✓	Win32 and Linux systems	attackers OS activities, state-based
high	Honeywall [93]	2005	2009	✓	*compare Sebek*, CentOS	live bootable CD
high	HoneyBow [96]	2006	2007	✓	Win32 Systems	extraction of malware, state-based
high	Argos [92]	2006	2014	✓	Linux, Windows XP-7	0-day exploits identification, tainting
high	HIHAT [94]	2007	2007	✓	php-BB,-Nuke,-Shell,-Myadmin	PHP framework extension, state-based

- Usually very targeted
- We wanted something more general
- No fine-grained malware binaries, but traffic meta-data
- Inspiration from different honeypots, in particular from the **Dionaea honeypot**

HoneyPort Architecture

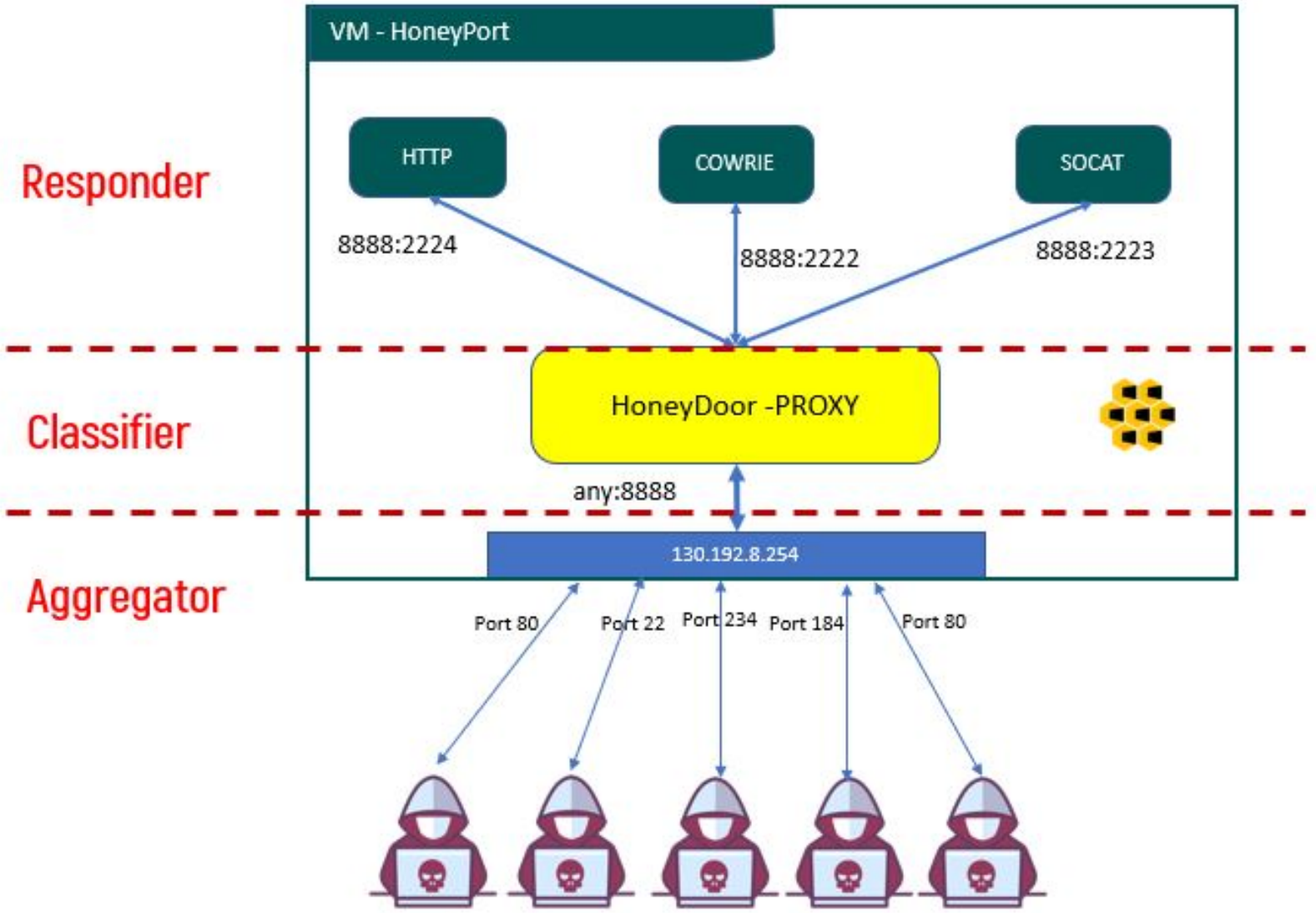


HoneyPort Architecture



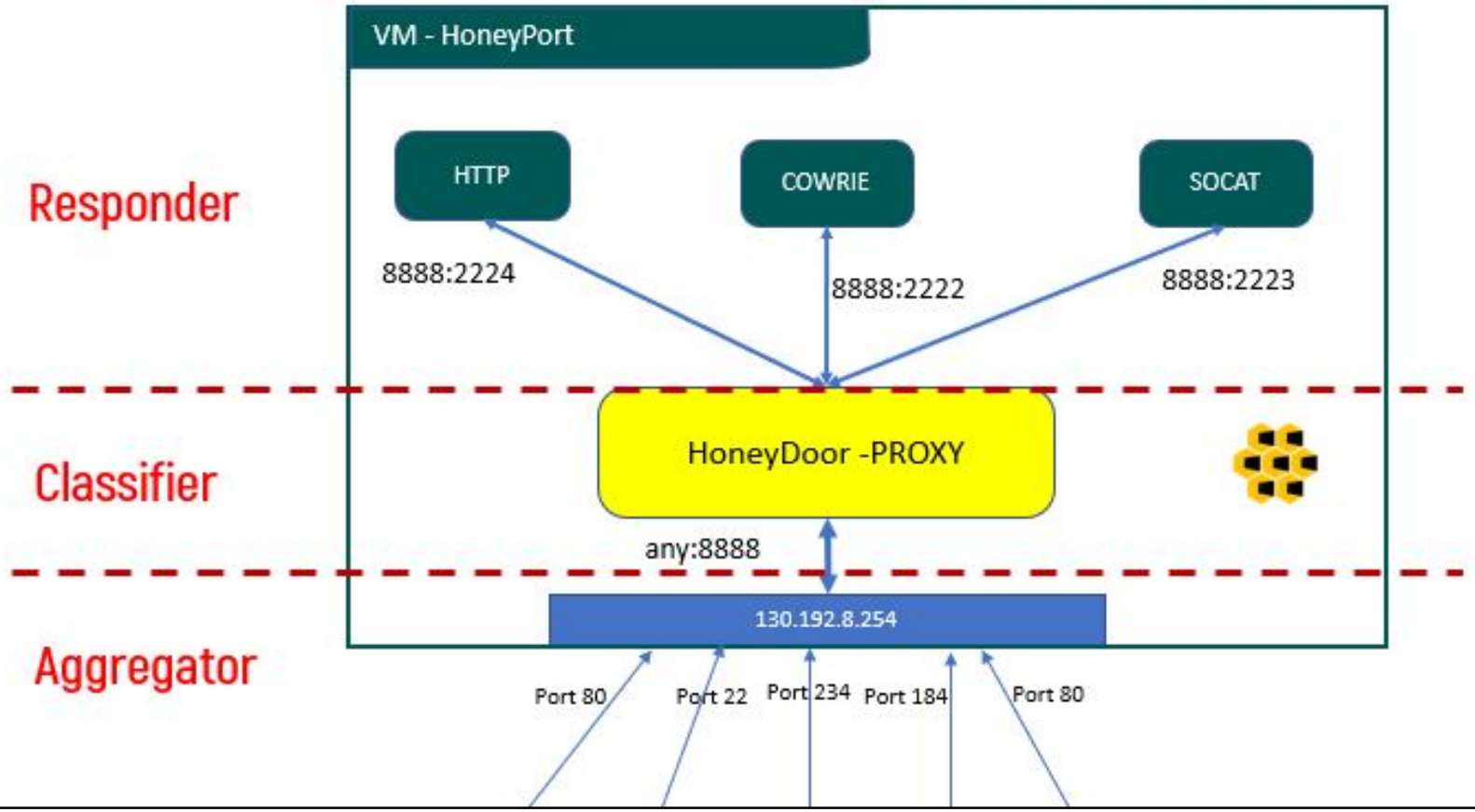
- L4 proxy (MiTM)

HoneyPort Architecture



- L4 proxy (MiTM)
- Keep context & packets
- Steer traffic to backends
- e.g, SSH on port 2222 will end in Cowrie
- e.g., web request on port 2222 will end on webserver

HoneyPort Architecture

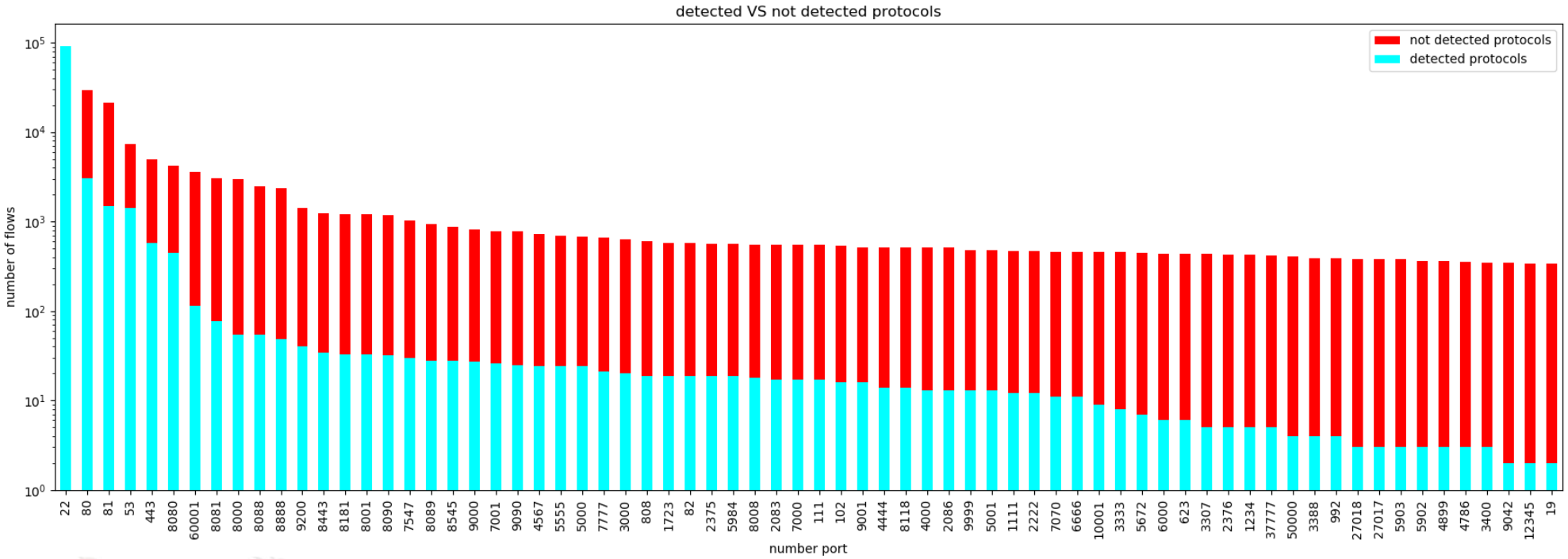


- L4 proxy (MiTM)
- Keep context & packets
- Steer traffic to backends
- e.g, SSH on port 2222 will end in Cowrie
- e.g., web request on port 2222 will end on webserver

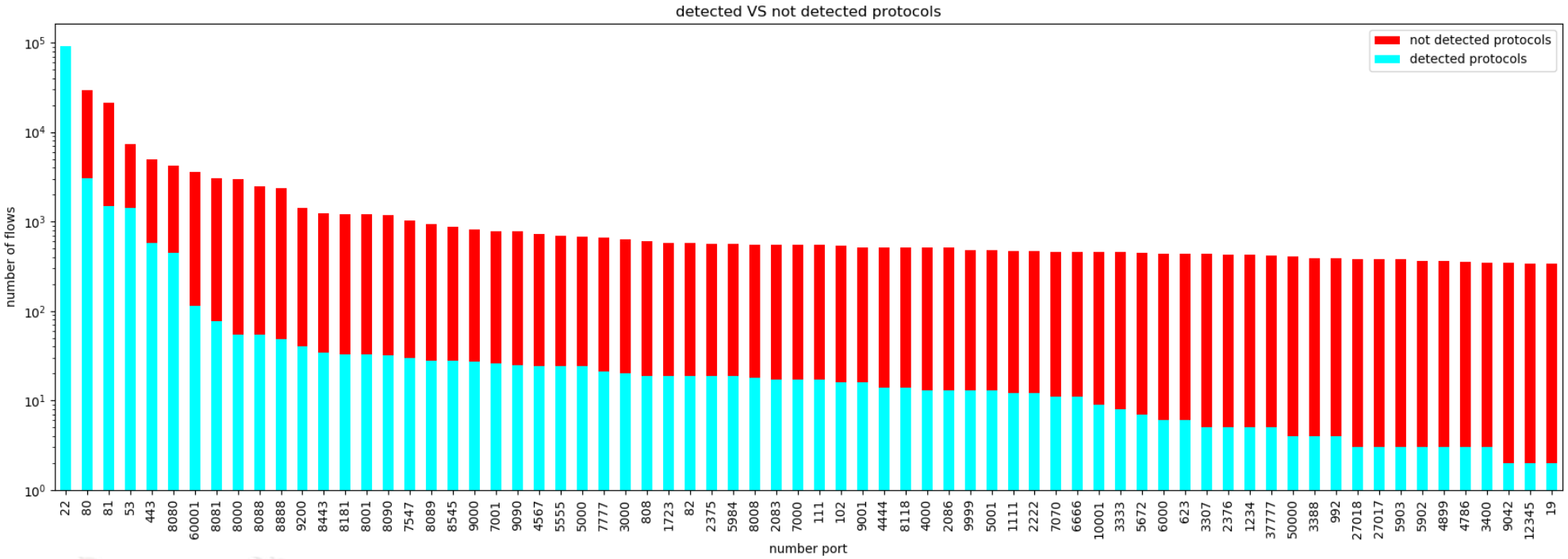
- Flexible deployment of the most “suitable” honeypot
- Rotate in the IP addresses in the space to avoid blacklisting
- Incrementally learn how to answer incoming packets

HoneyPort – Initial data

HoneyPort – Initial data

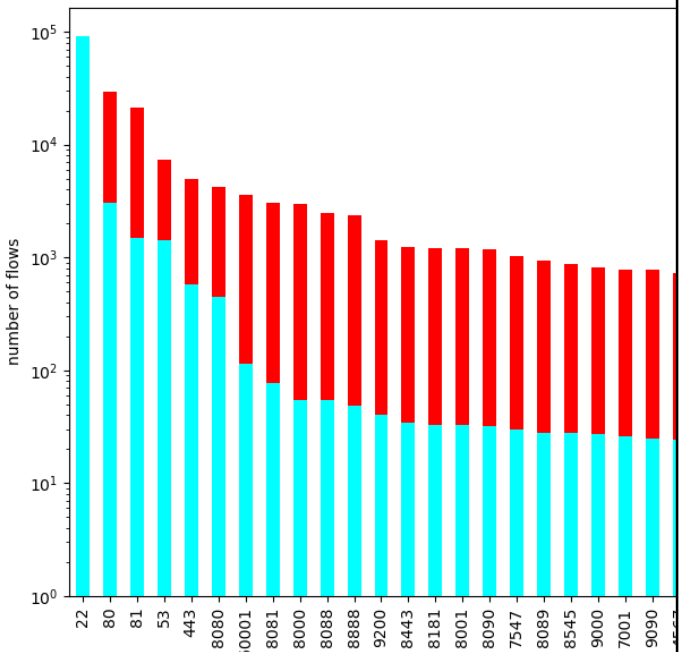


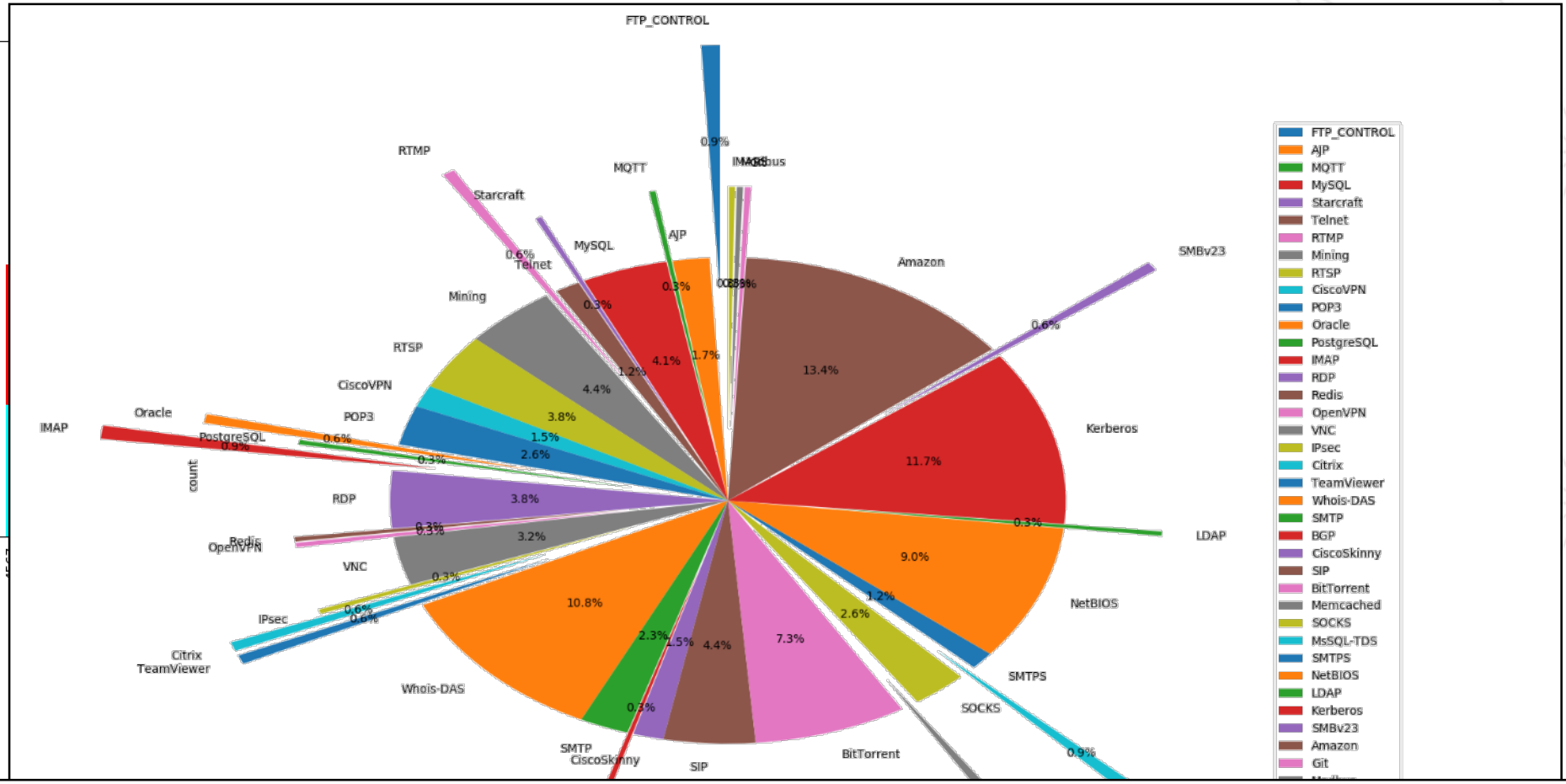
HoneyPort – Initial data



- Initial analyses based on first packets (max 1 after the TCP handshake)
  - Protocol fingerprints from NPI (with some weird categories inside)

HoneyPort – Initial data



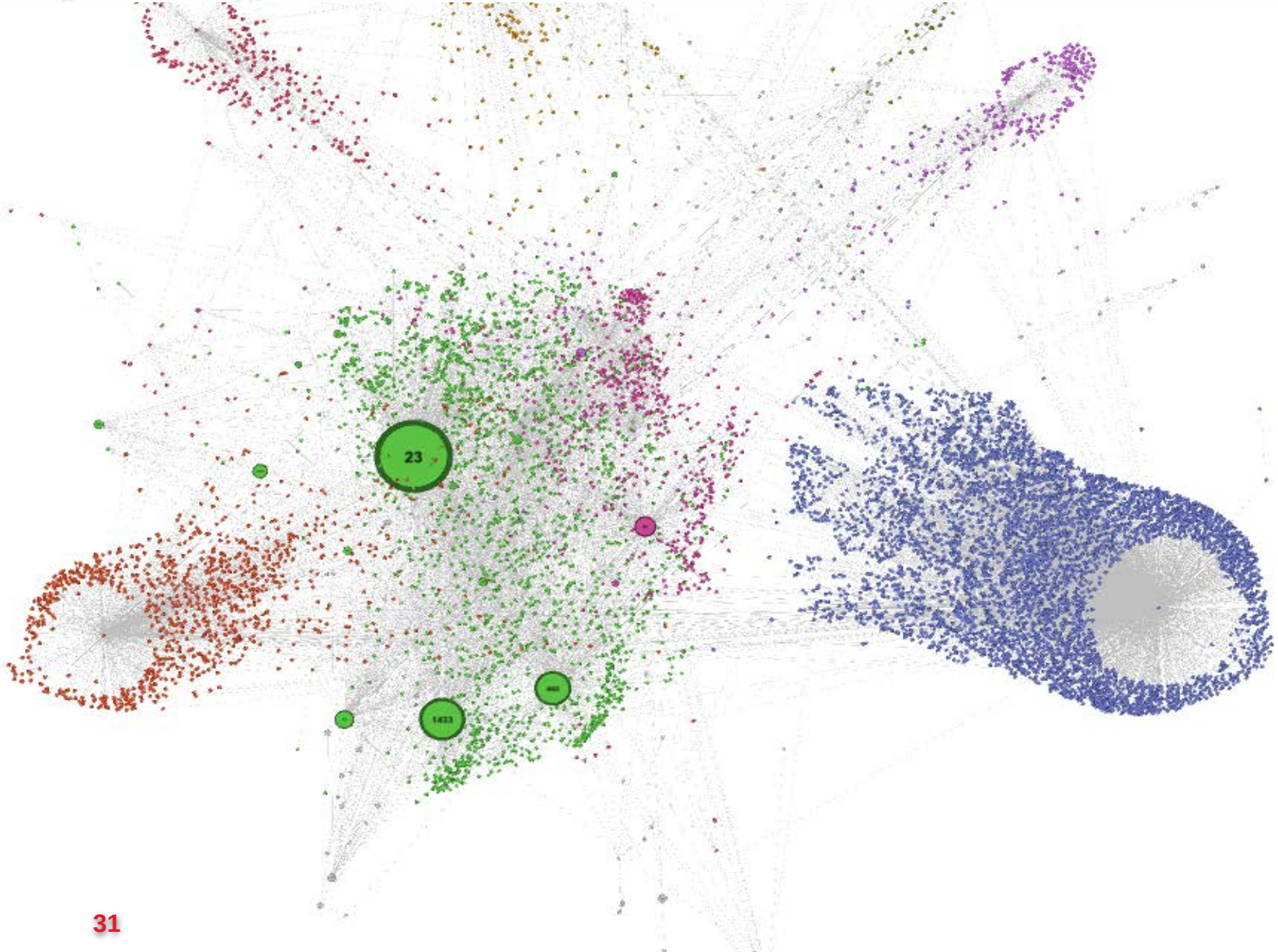


- Initial analyses based on first packets (max 1 after the TCP handshake)
  - Protocol fingerprints from NPI (with some weird categories inside)

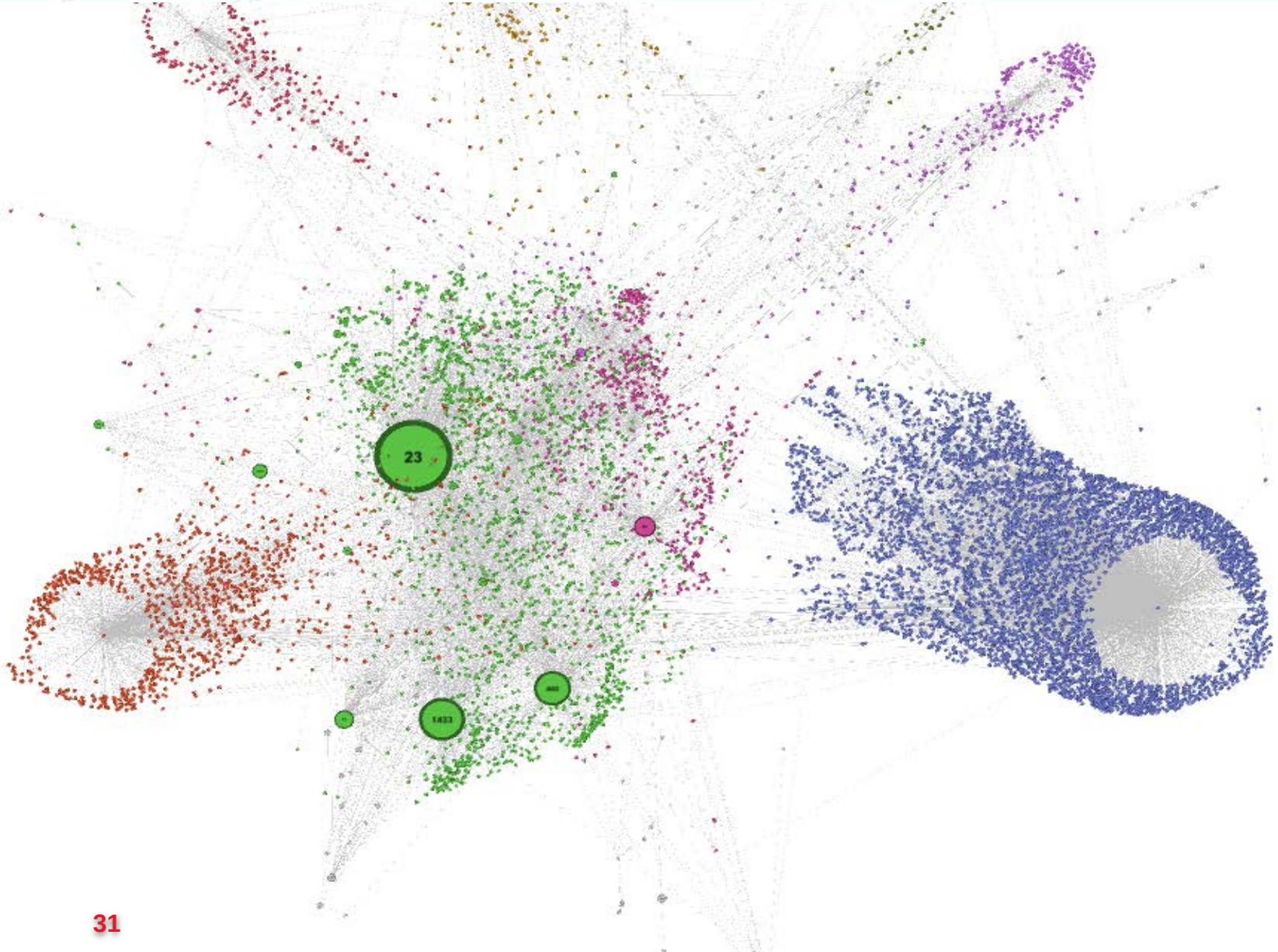
Many open points/questions

- **Match the scanner with follow-up flows**
  - Not always the same IP address
- Temporal effects
  - The more you answer, the more you get
  - Quality of what you get? (becoming are a known honeypot)
- How to match honeypot traffic with darknet traffic?
- For many protocols, what to answer is not clear yet
  - What should I answer to a DNS request?
- Backscattering/spoofed identification

Grouping Origins (ongoing)

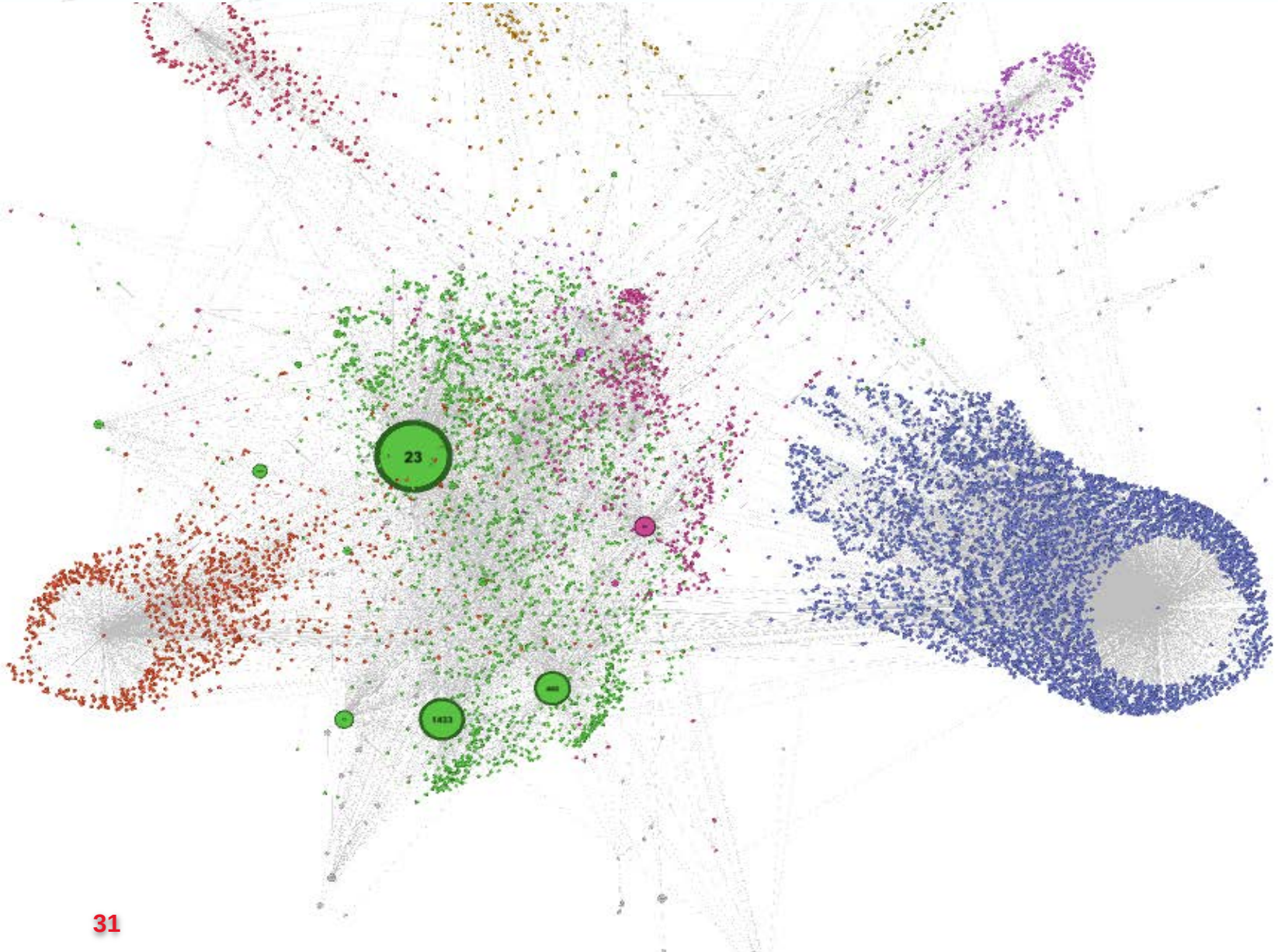


Grouping Origins (ongoing)



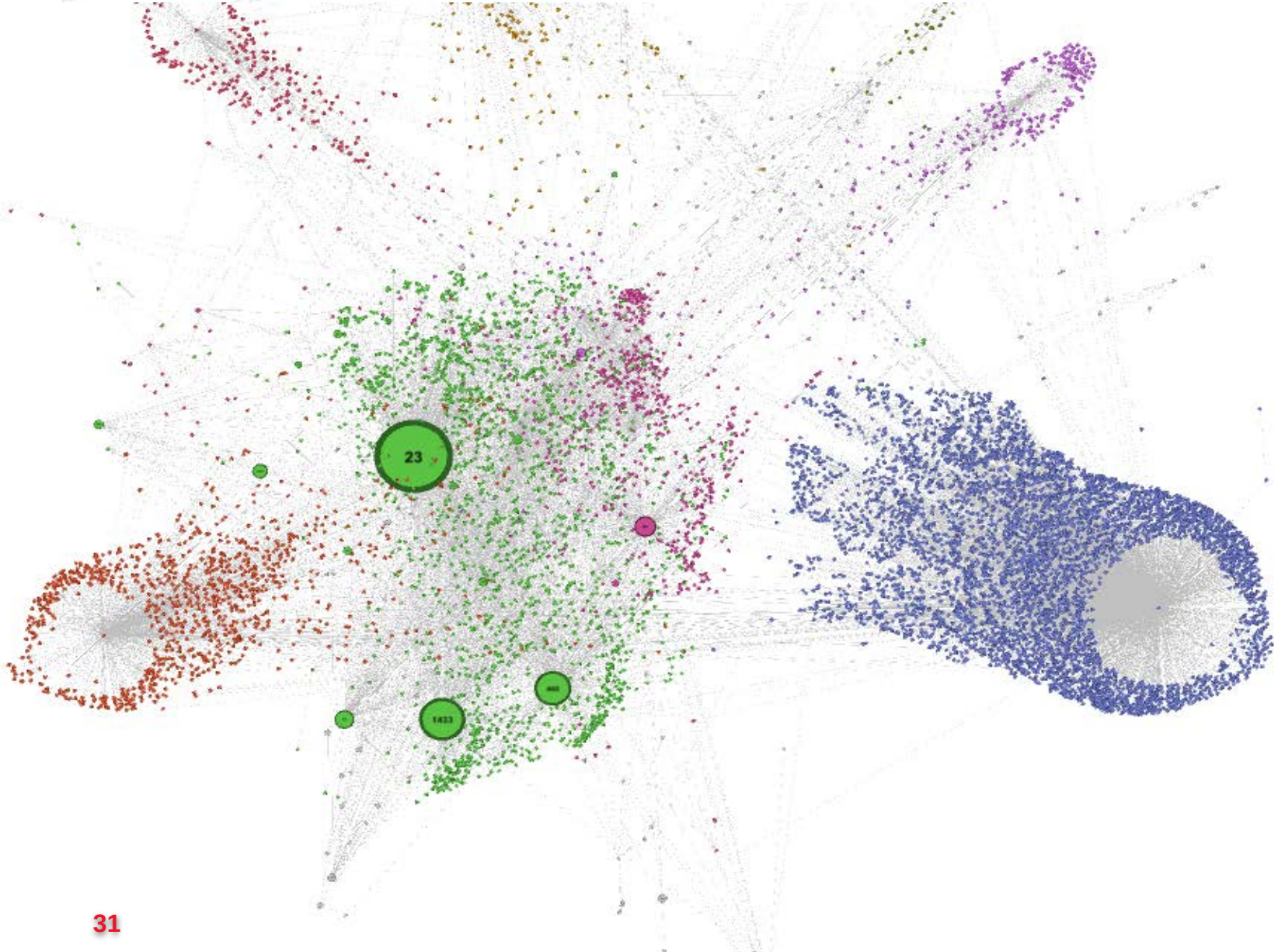
- From different darknets

Grouping Origins (ongoing)



- From different darknets
- Groups of ASes doing similar activity simultaneously

Grouping Origins (ongoing)



- From different darknets
- Groups of ASes doing similar activity simultaneously
  - e.g., port scans
  - e.g., groups that send packets to single port
  - e.g., groups sending few packets everywhere (e.g., backscaterring)


Perguntas
Fragen
Domande
Galdera
Otázky
Questions
Spørgsmål
Pertanyaan
kysymykset
Frågor
Spørsmål
Cwestiynau
вопросы
Preguntes
Sorular
Въпроси
Vragen
Pytania