TEAM CYMRU

Team Cymru

Community Services

Brian Davenport

Presenter: Brian Davenport

- Solutions Engineer with Team Cymru, supporting community services.
- Training, Configuration, Demo’s whatever you need!
- Contact Info :
  - Email: bdavenport@cymru.com
  - LinkedIn: https://www.linkedin.com/in/briandavenport1/
  - Calendar: https://calendly.com/bdavenport-3

Team Cymru (pronounced come-ree)

TEAM CYMRU

Founded in 2005

Mission:

To save and improve human lives.

- Free services to ISPs, hosting providers and CSIRTs
- Unmatched eco-system of data sharing and collaboration partnerships worldwide
- Work with 130+ CSIRT teams in 86+ countries
- Relied on by many security vendors, Fortune 100 companies, and public sector teams.

Community Services

TEAM CYMRU

Restricted Events

Underground Economy

Regional Internet Security Events (RISE)

Free Tools / Services

- NimbusTM
- BOGON Reference
- Malware Hash Registry
- Unwanted Traffic Removal Service
- Dragon News Bytes (threat news feed)

CSIRT Assistance

137 CSIRT Teams

52% of IPV4

75% of IPV6

NimbusTM

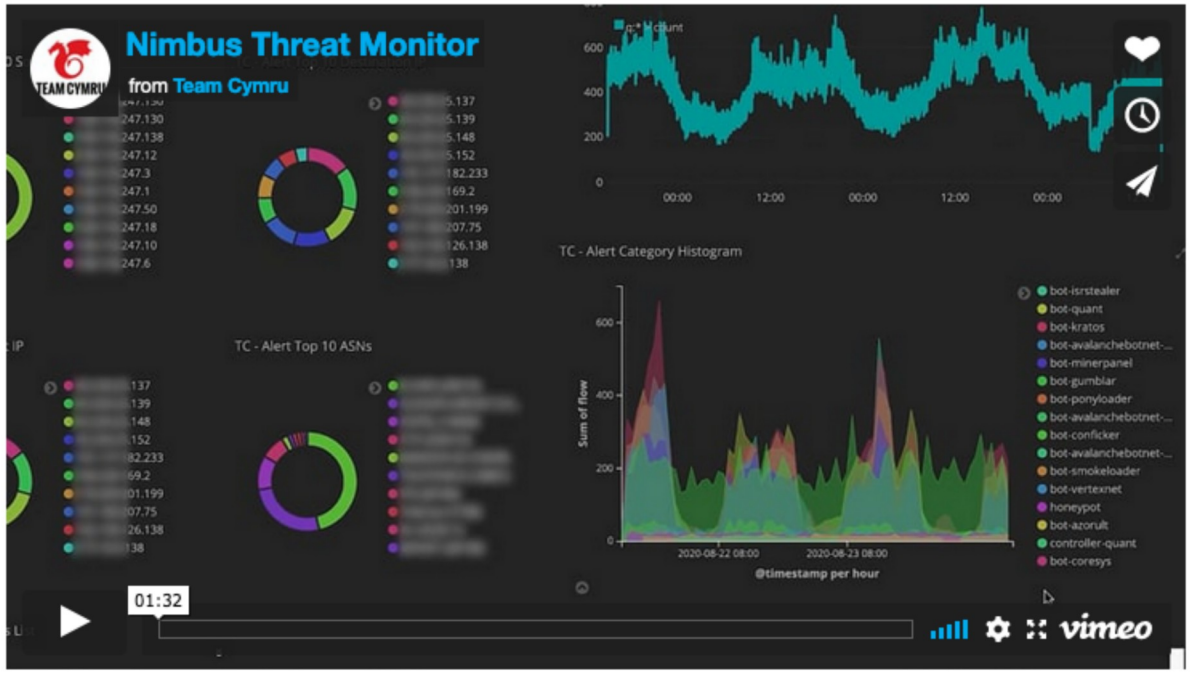
- Cloud based collector, built on Elastic / Kibana.
- Free to use for ISPs, hosting providers and CSIRTs.
- Correlates flow data with reputation feeds.
- **Sign Up Today:** https://team-cymru.com/community-services/nimbus-threat-monitor/

Join thousands of networks around the world.

Partner with Team Cymru to improve your network security and contribute to the global effort to secure the Internet as a whole. Nimbus Threat Monitor works by correlating your network flows with our world-class IP Reputation threat intelligence. When you share your network traffic metadata with us, we pool it with data from thousands of networks worldwide and mine it to identify cyber threat activity. In turn, we give you near-real-time threat detection at no cost to you.

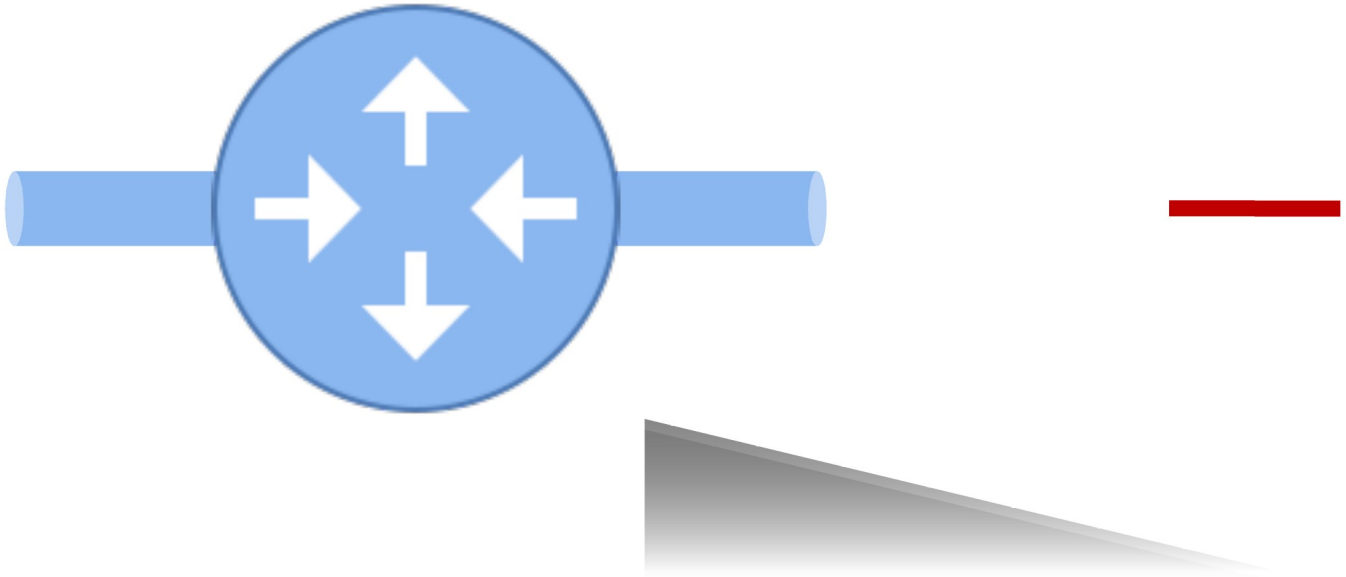
Nimbus Data Sheet

GET STARTED

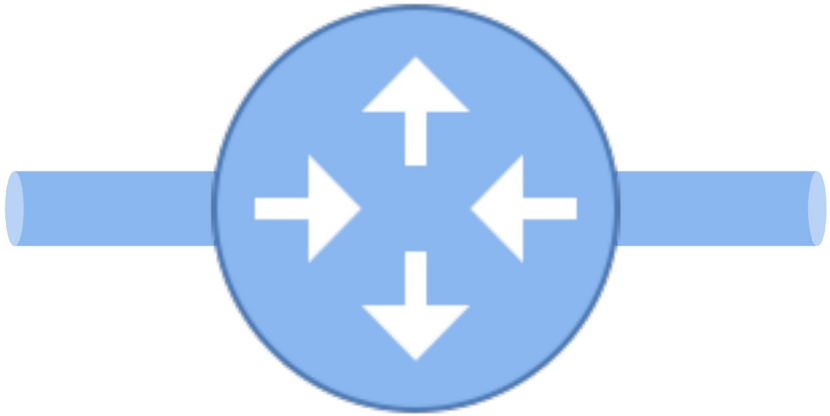


Nimbus Threat Monitor from Team Cymru on Vimeo.

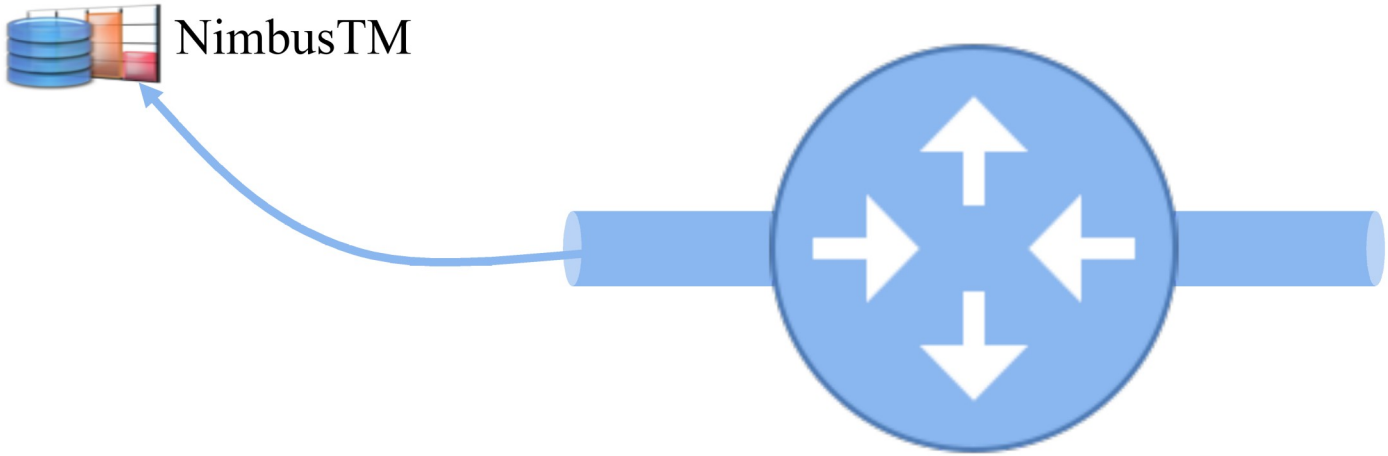
Flow Data – How it works…



Destination IP	Source IP	Destination Port	Source port	Source Interface	Protocol	Bytes
8.8.8.8	1.1.1.1	80	65000	1	TCP	100



Destination IP	Source IP	Destination Port	Source port	Source Interface	Protocol	Bytes
8.8.8.8	1.1.1.1	80	65000	1	TCP	600
4.4.4.4	2.2.2.2	80	64500	1	TCP	50



Destination IP	Source IP	Destination Port	Source port	Source Interface	Protocol	Bytes
8.8.8.8	1.1.1.1	80	65000	1	TCP	600
4.4.4.4	2.2.2.2	80	64500	1	TCP	50

NimbusTM Data Enrichment

TEAM CYMRU

Destination IP	Source IP	Destination Port	Source port	Source Interface	Protocol	Bytes
8.8.8.8	1.1.1.1	80	65000	1	TCP	100

Destination IP	Destination ASN	Source IP	Source ASN	Destination Port	Source port	Source Interface	Protocol	Bytes	Alert IP	Alert_ASN	Alert Signature	Confidence
8.8.8.8	**GOOGLE, US (151169)**	1.1.1.1	**BrianCo (65536)**	80	65000	1	TCP	100	1.1.1.1	**BrianC0 (65536)**	**Brian Malware**	**100**

TC - Flow Sources (Stat)

[TC - Alert] Top Alert IP

alert_signature: Descending	Sum of flow	Sum of bytes	Sum of pkts
bot-gumblar	25.187 k	5.869GB	3.805 m
bot-smokeloader	2.27 k	240.279MB	121.789 k
bot-conficker	553	280.31MB	220.132 k
scanner	421	28.197KB	599
bot-ponyloader	358	3.034MB	3.95 k
bot-vertexnet	306	133.275MB	79.652 k
bot-kasidet	76	57.091MB	26.485 k
bot-lokibot	72	295.552KB	663
honeypot	36	4.817KB	37
bot-amadey	18	48.864KB	161

Destination ASN

AMAZON-02 (16509)

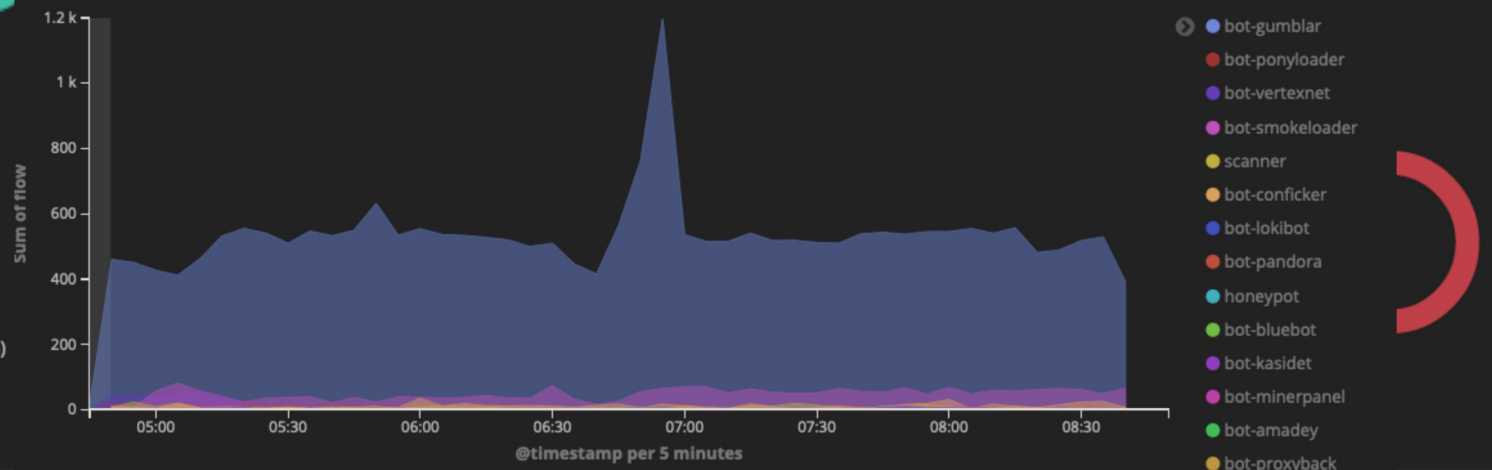
BrianCo(65536)

Identi

rend

[TC - Alert] Alerts Over Time

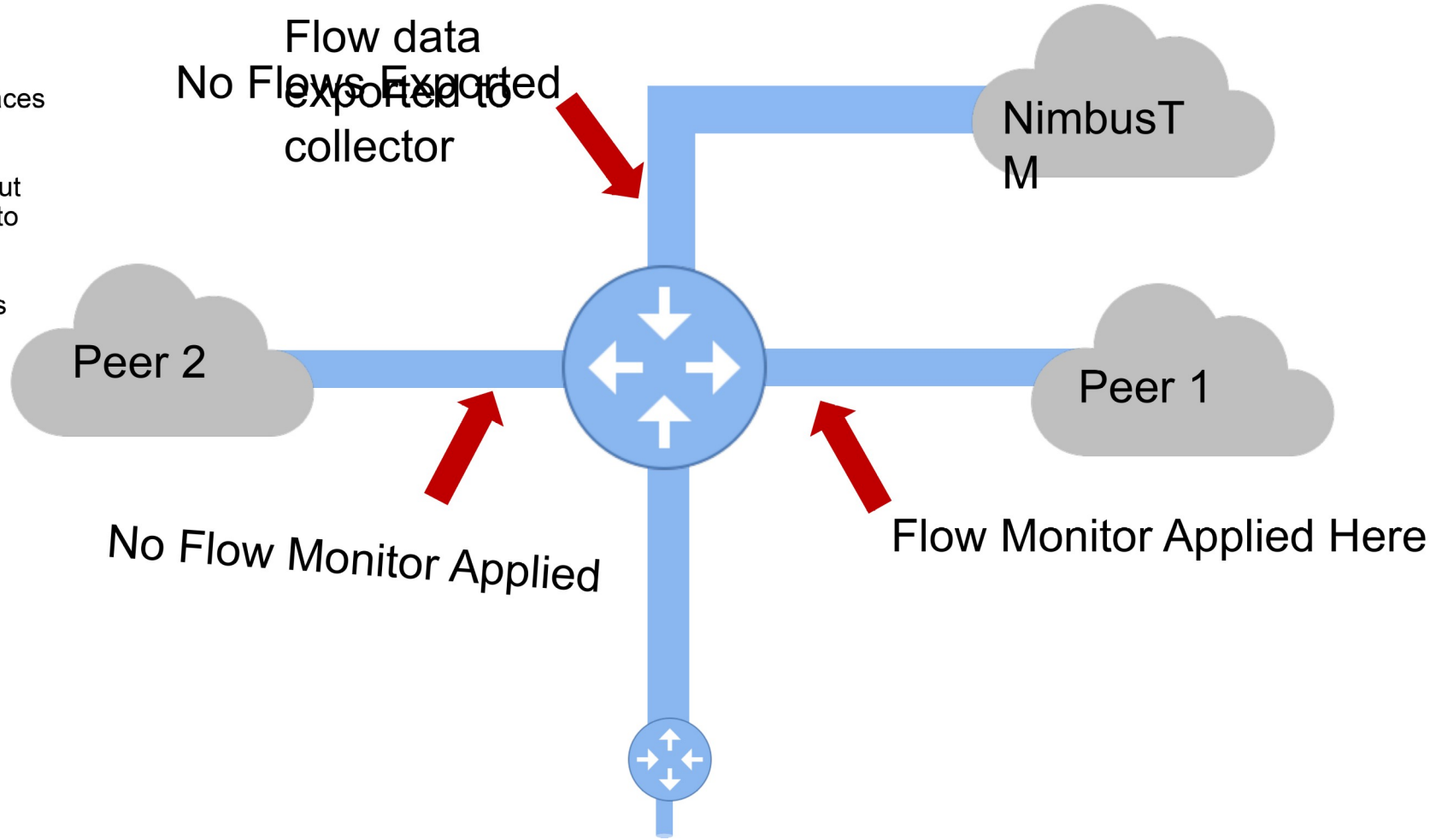
[TC - Alert] Category Histogram



TEAM-CYMRU (23028) (100%)

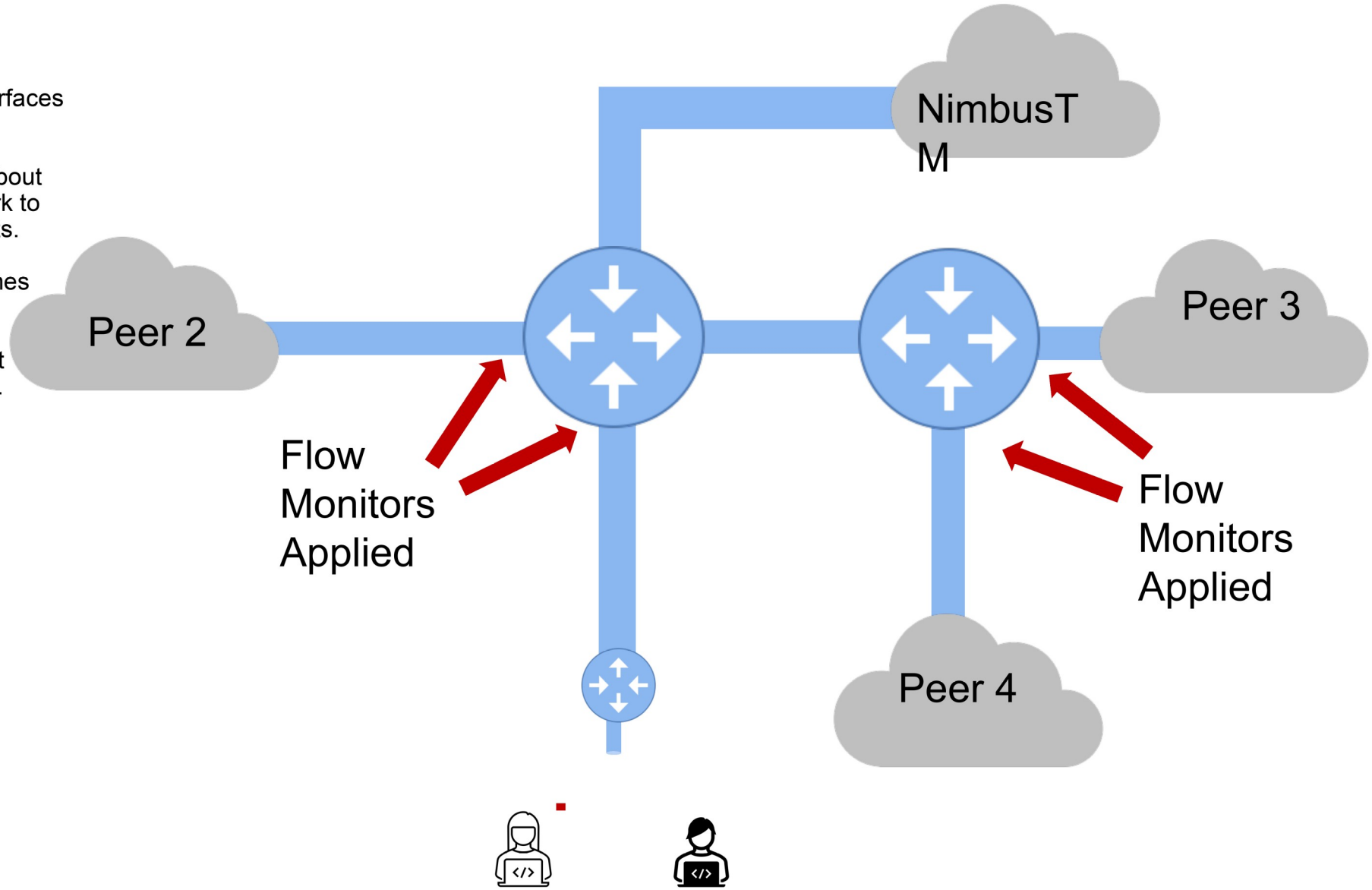
Where to gather data from?

- Flow monitors are applied to the interfaces you want to observe traffic for
- When applying flow monitors think about how traffic flows through your network to make sure you gather at funnel points.
- Configuring IPv6 Monitoring sometimes requires additional configuration



Where to gather data from?

- Flow monitors are applied to the interfaces you want to observe traffic for
- When applying flow monitors think about how traffic flows through your network to make sure you gather at funnel points.
- Configuring IPv6 Monitoring sometimes requires additional configuration.
- Equally important to think about what network devices traffic flows through.



UTRS

TEAM CYMRU

Unwanted Traffic Removal Service

- Like RTBH, but:
  upstream and **global**
- Over 1,200 participating networks
- Reduces unwanted traffic hitting you and others

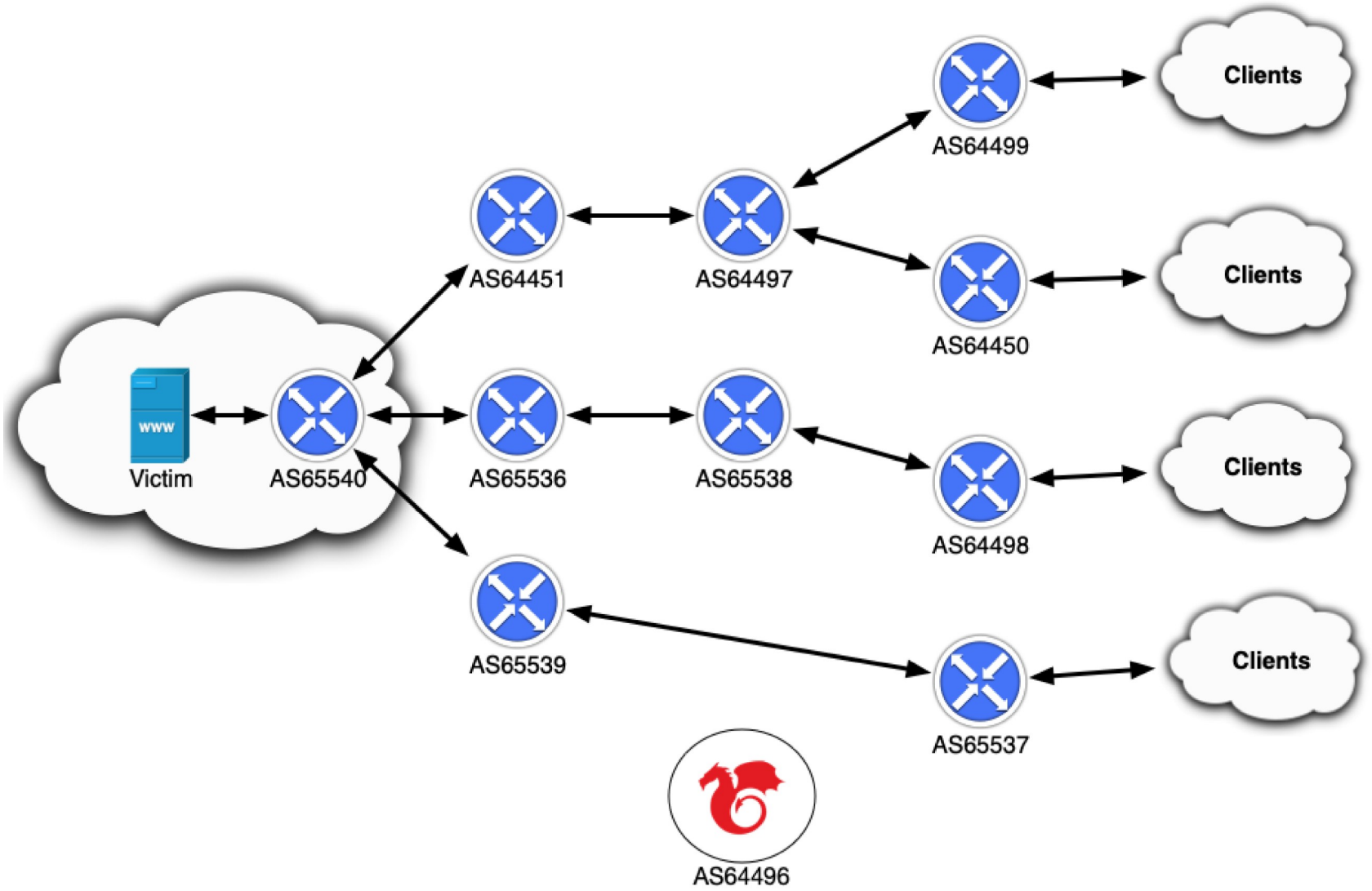
UTRS

BGP based triggers, with two basic rules:

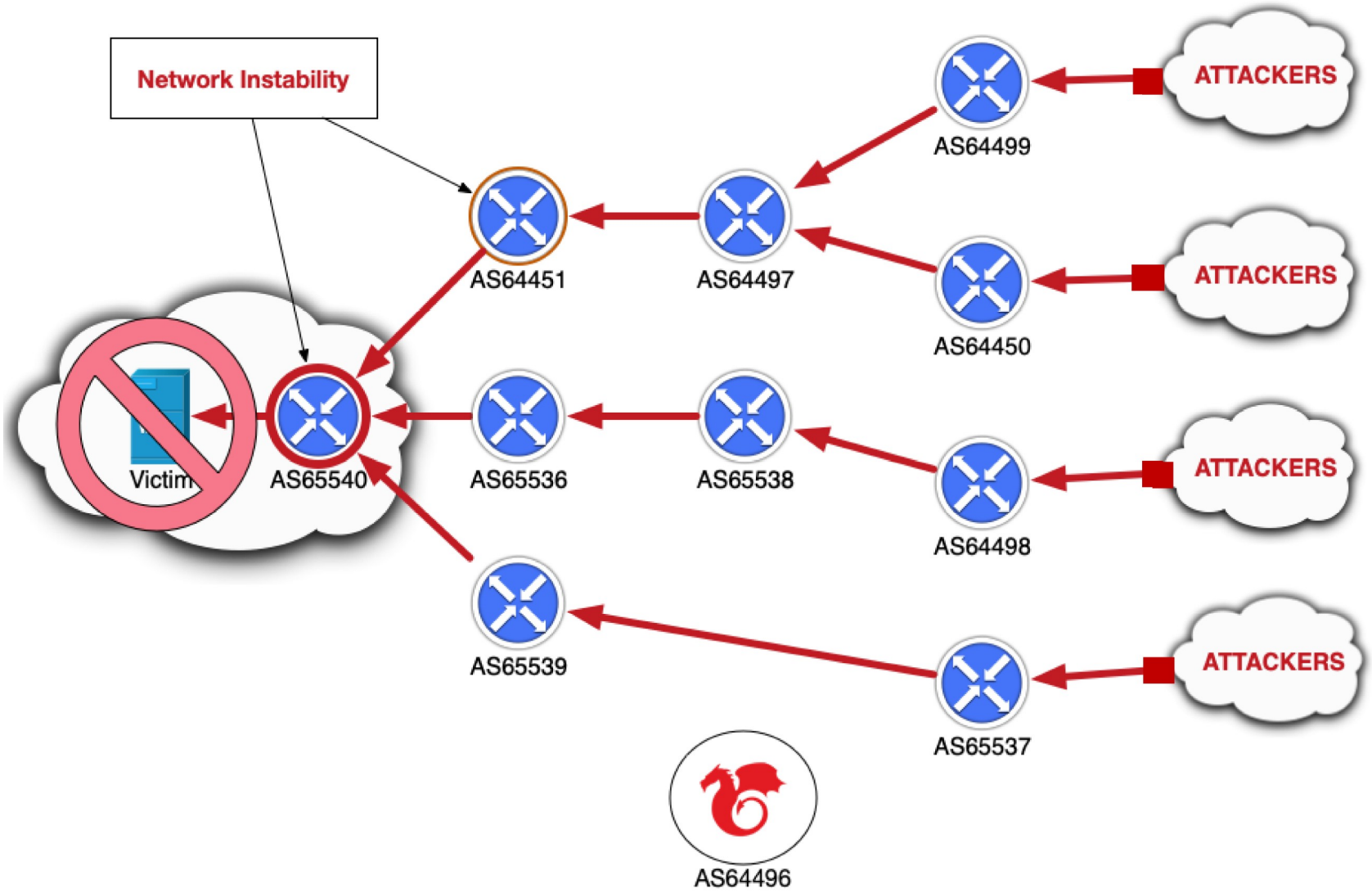
- Accepts only IPv4 /32 advertisements for addresses within prefixes you originate
- You agree to null route traffic to routes received from UTRS

- 2.0 new features
- Add FlowSpec support
- Add RPKI validation (Mitigation service friendly)
- Add support for IPv6
- Allow larger prefixes (up to IPv4 /25, IPv6 /49)

UTRS

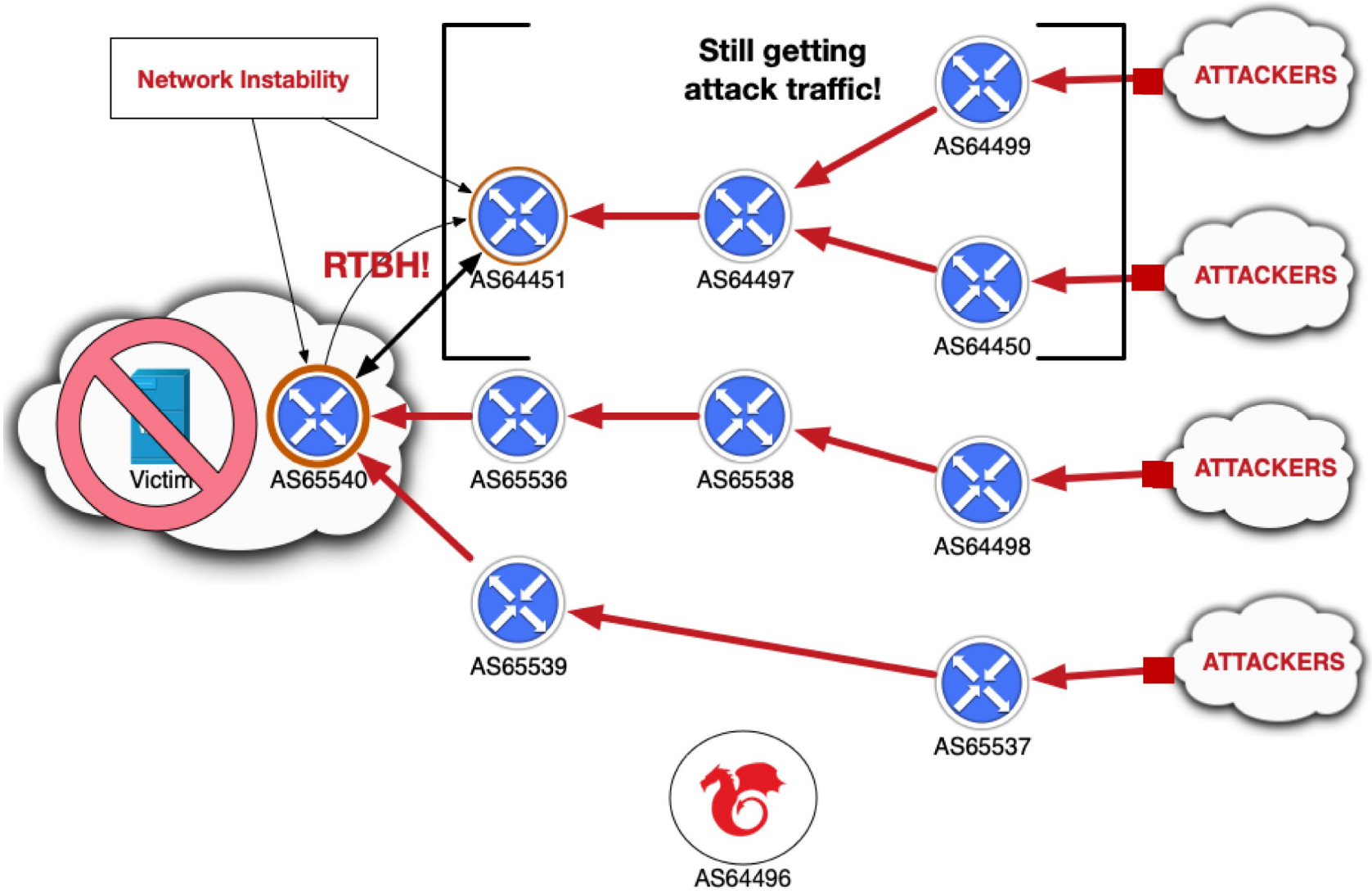

Clients
AS64499
AS64451
AS64497
Clients
AS64450
www
Victim
AS65540
AS65536
AS65538
Clients
AS64498
AS65539
Clients
AS65537
AS64496

UTRS


Network Instability
ATTACKERS
AS64499
AS64451
AS64497
ATTACKERS
AS64450
Victim
AS65540
AS65536
AS65538
ATTACKERS
AS64498
AS65539
ATTACKERS
AS65537
AS64496

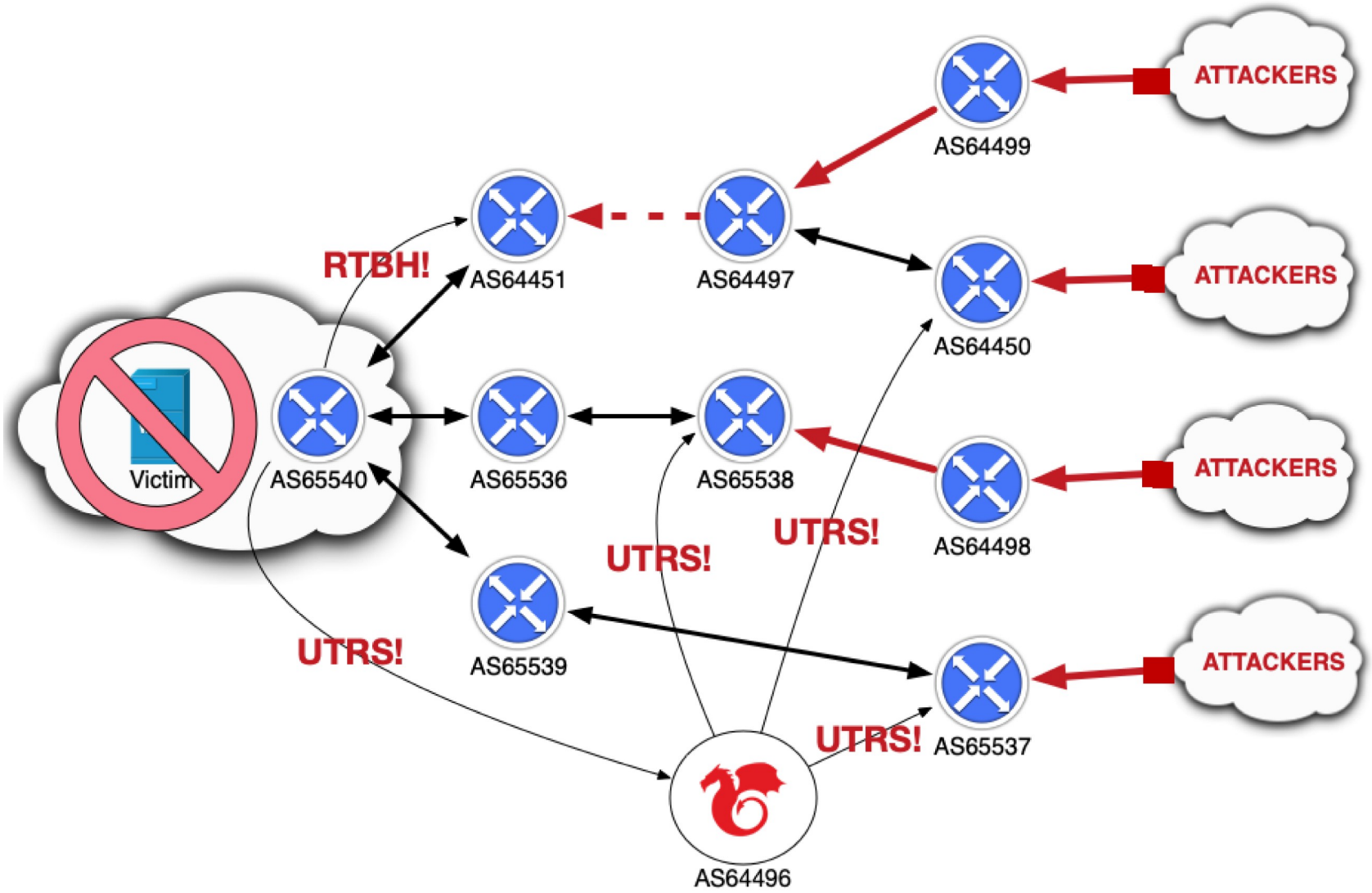
UTRS

TEAM CYMRU



UTRS

TEAM CYMRU



CAP

CSIRT Assistance Program (CAP)

- Free reputation data
- Contains our filtered set of threat intelligence
  - Specific to “jurisdiction”
- Available to Regional and National CSIRTs only

Other Services

TEAM CYMRU

- IP to ASN Mapping:
  https://team-cymru.com/community-services/ip-asn-mapping/
- Malware Hash Registry:
  https://team-cymru.com/community-services/mhr/
- Dragon News Bytes:
  https://team-cymru.com/community-services/dnb/

Thank you.

CYMRU.COM | 847-378-3300