TEAM CYMRU™

UTRS Roadmap

Unwanted Traffic Removal Service
v2.0 and beyond

James Shank
Chief Architect, Community Services
jshank@cymru.com

Agenda

- What is Team Cymru
- UTRS v1 and what “UTRS” is…
- UTRS v2 and introduce BGP FlowSpec
- UTRS v3
- Nimbus Threat Monitor and other Community Services

Team Cymru (pronounced come-ree)

Mission: To Save and Improve Human Lives

- Founded 2005
- Free services to ISPs, hosting providers and CSIRTs
- Work with 138+ CSIRT teams in 86+ countries
- Free tools used millions of queries per day

Community Services

Restricted Events

Underground Economy

Regional Internet Security Events (RISE)

Free Tools / Services

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

CSIRT Assistance

138 CSIRT Teams

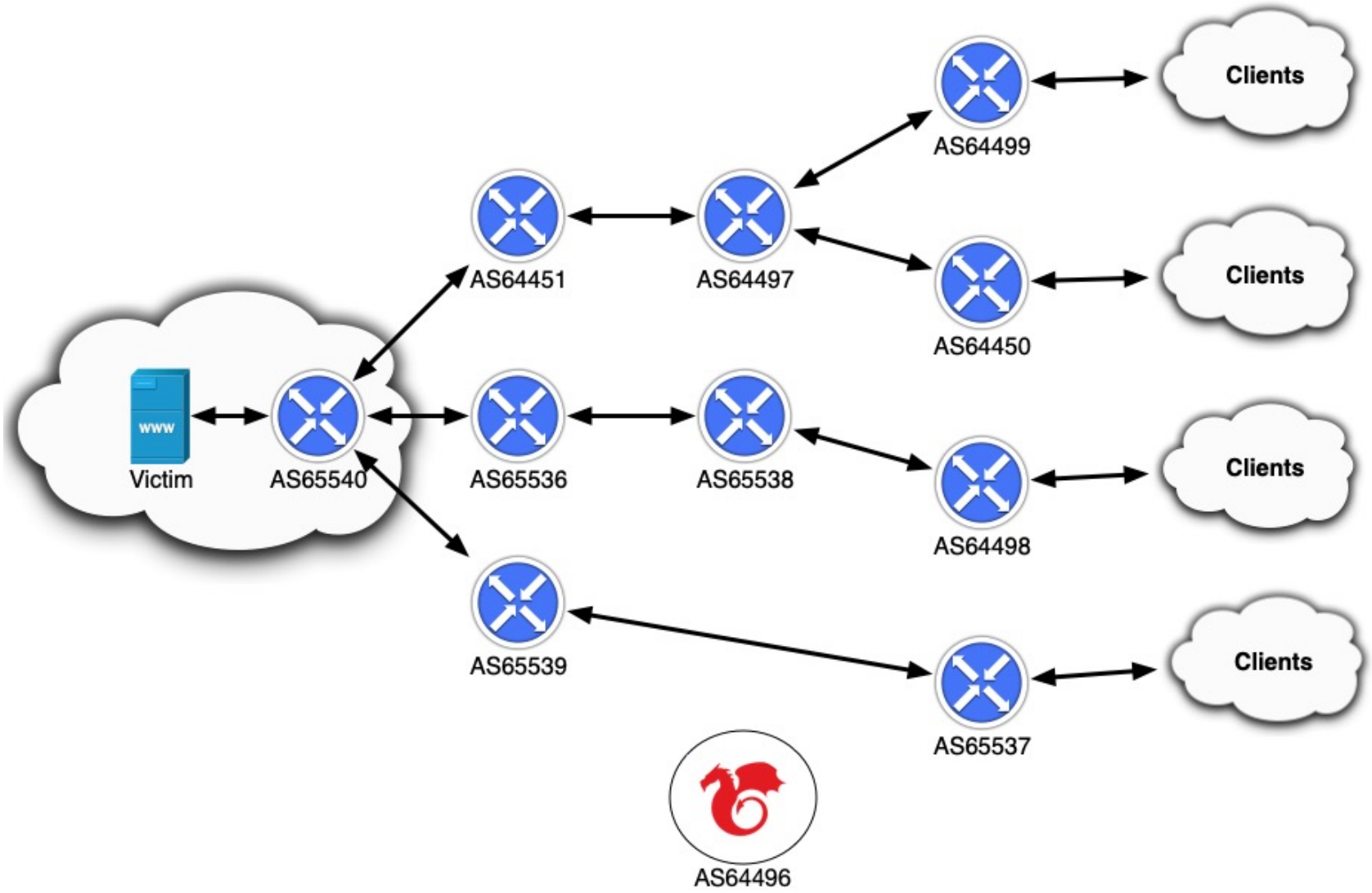
52% of IPV4

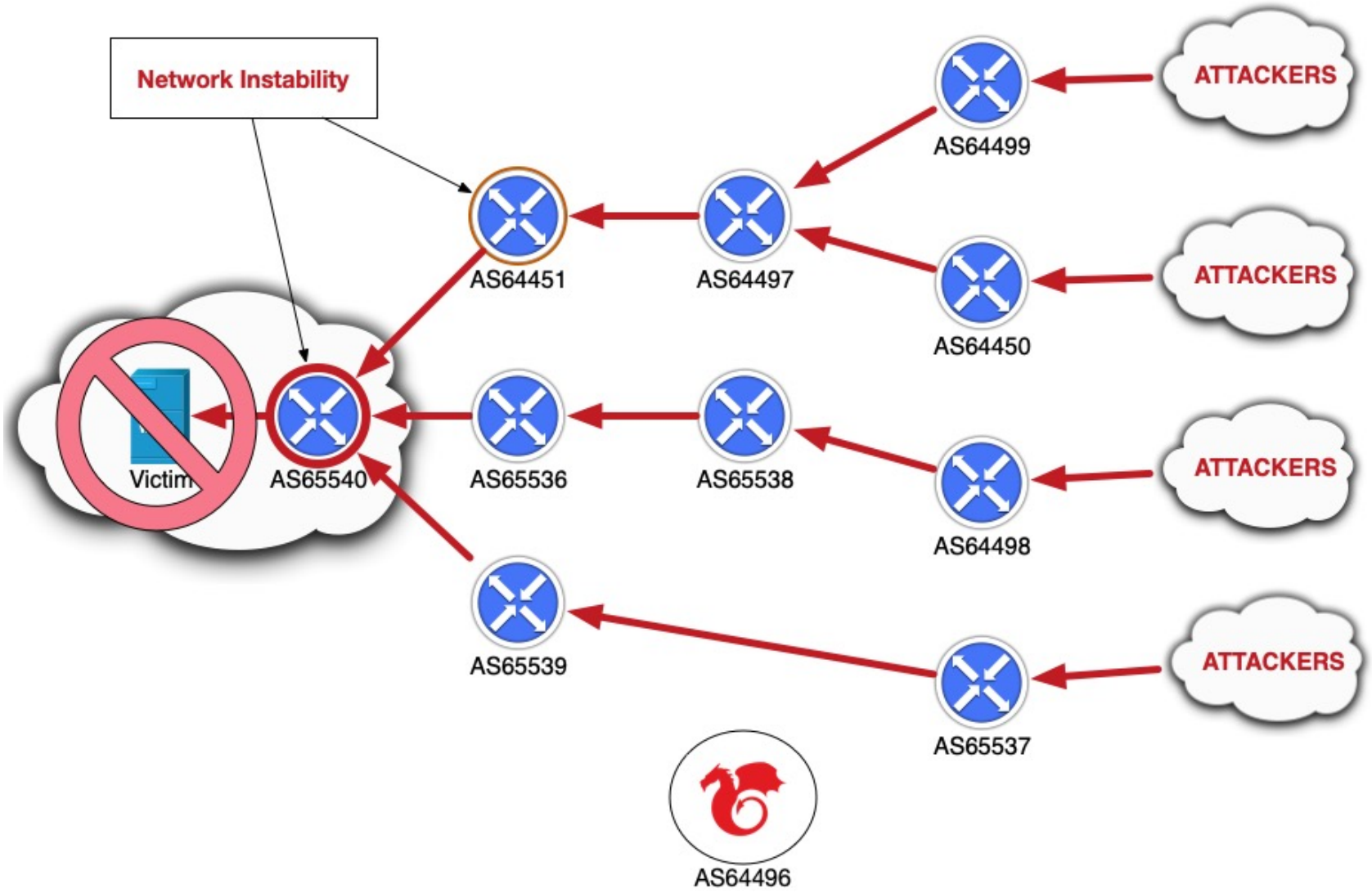
75% of IPV6

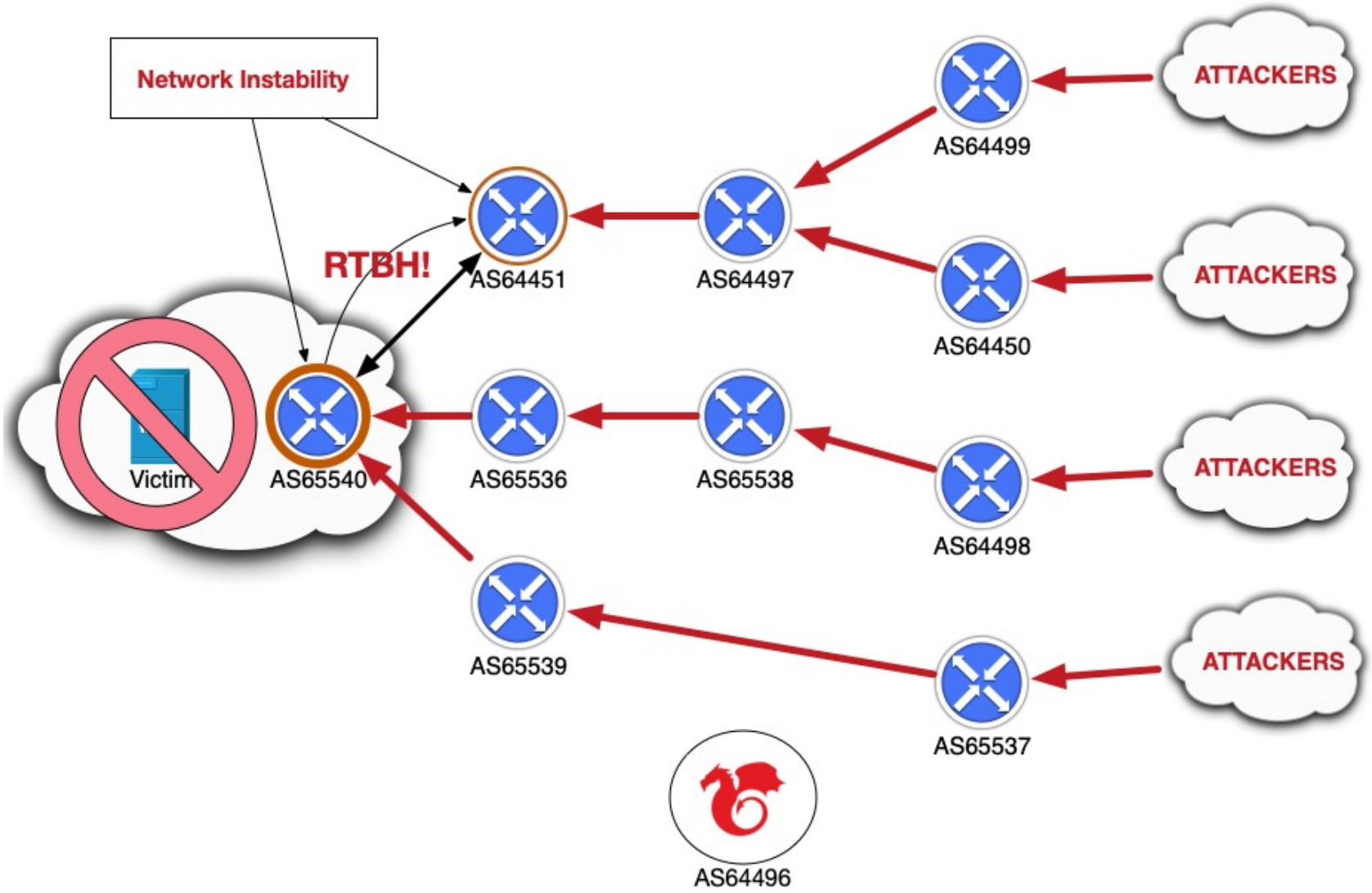
What is UTRS?

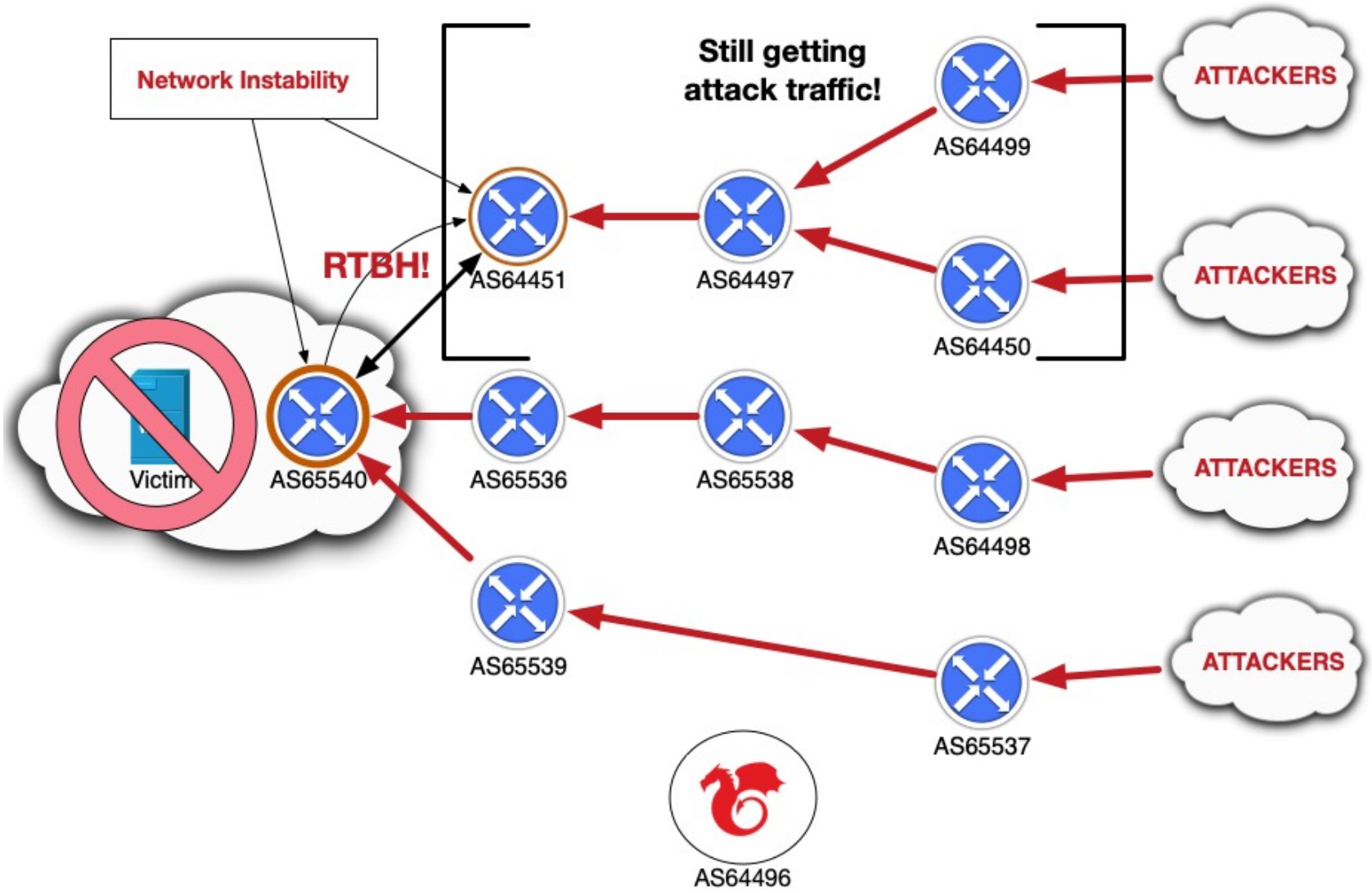
Unwanted Traffic Removal Service

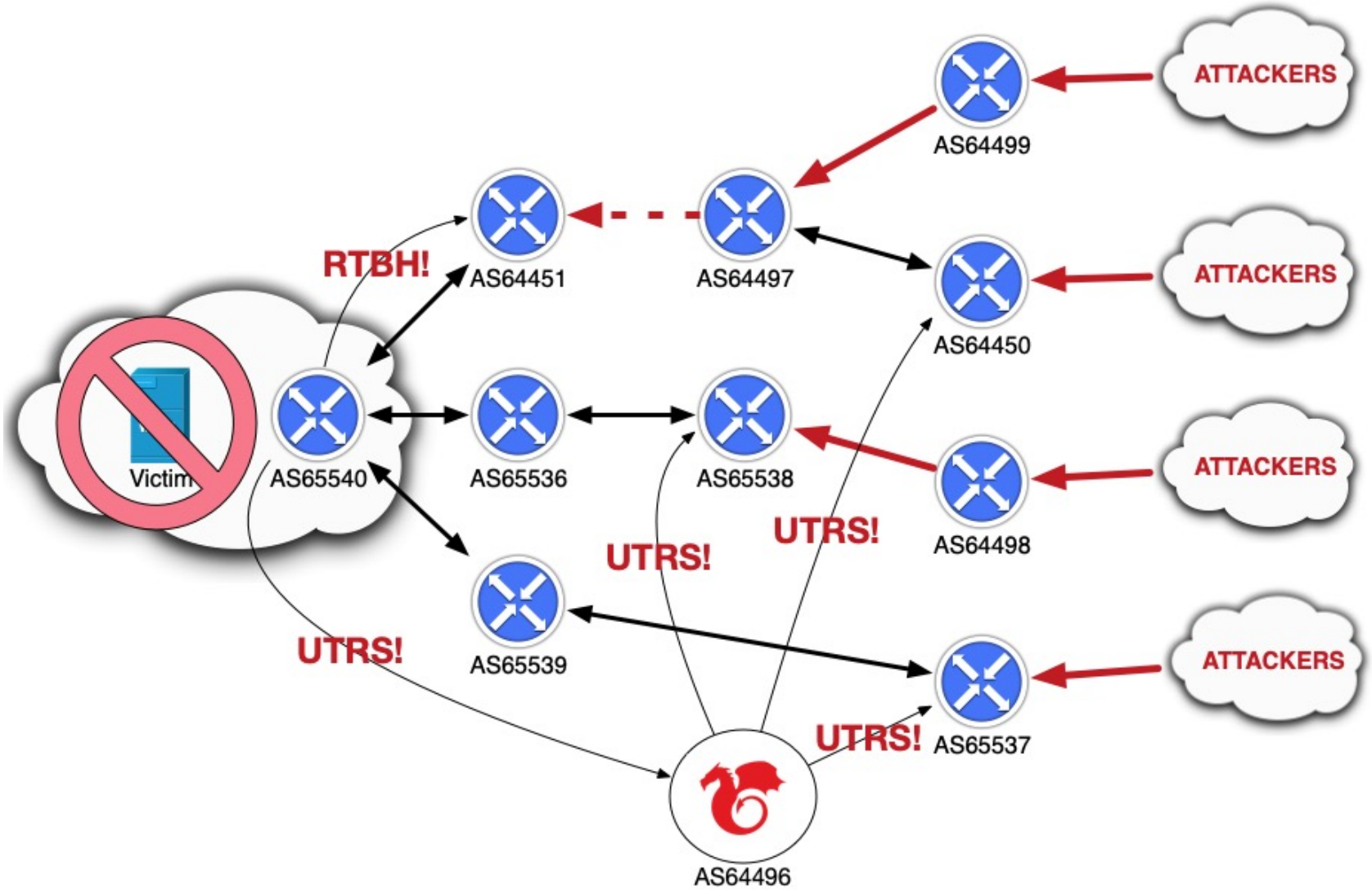
- Uses BGP, but to send “distress” signal
- Builds on RTBH (Remote Triggered Black Hole)
- Victim network asks TC to ask all our UTRS peers to *stop sending traffic*
  - *Much wider range*
- Completes the attack – at least in Version 1


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


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


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


Network Instability
Still getting
attack traffic!
RTBH!
AS64451
AS64497
AS64499
AS64450
ATTACKERS
ATTACKERS
Victim
AS65540
AS65536
AS65538
AS64498
ATTACKERS
AS65539
AS65537
ATTACKERS
AS64496


ATTACKERS
AS64499
RTBH!
AS64451
AS64497
ATTACKERS
AS64450
Victim
AS65540
AS65536
AS65538
ATTACKERS
AS64498
UTRS!
UTRS!
UTRS!
AS65539
ATTACKERS
AS65537
UTRS!
AS64496

UTRS v1.0

The live, production version

- Distributes RTBH requests
- IPv4 only
- Allows only /32s to be advertised
- 1206 configured sessions
- 1024 configured peers
- Free to use

UTRS v2.0

Coming VERY soon

- Adds IPv6 support!
- Adds ”larger prefix” support to fight carpet bombing
  - /25 for IPv4 and /49 for IPv6
- Allows RPKI validation for authorizing advertisements
  - Friendly to DDoS mitigation providers
- Adds “safe” BGP FlowSpec support!
  - This is a BIG deal, gets rid of “completing the attack”

BGP Flow Specification

RFC 8955

- Defines well known community

VERY powerful and enumerative!

- Rate limit, redirect, tag, etc
- Full suite of Boolean operators
- Specify prefixes, chain rules

And can crater routers

Many networks don’t accept it from peers

”Safe” BGP FlowSpec

Lab tested, network operator approved (in some cases)

MUST specify

- Source CIDR XOR Destination CIDR

MAY specify any combination of the following:

- Protocol (Explicit integers only)
- Source Port (Explicit integers only)
- Destination Port (Explicit integers only)

MUST set action to DROP (traffic-rate 0)

UTRS v3.0

Looking ahead

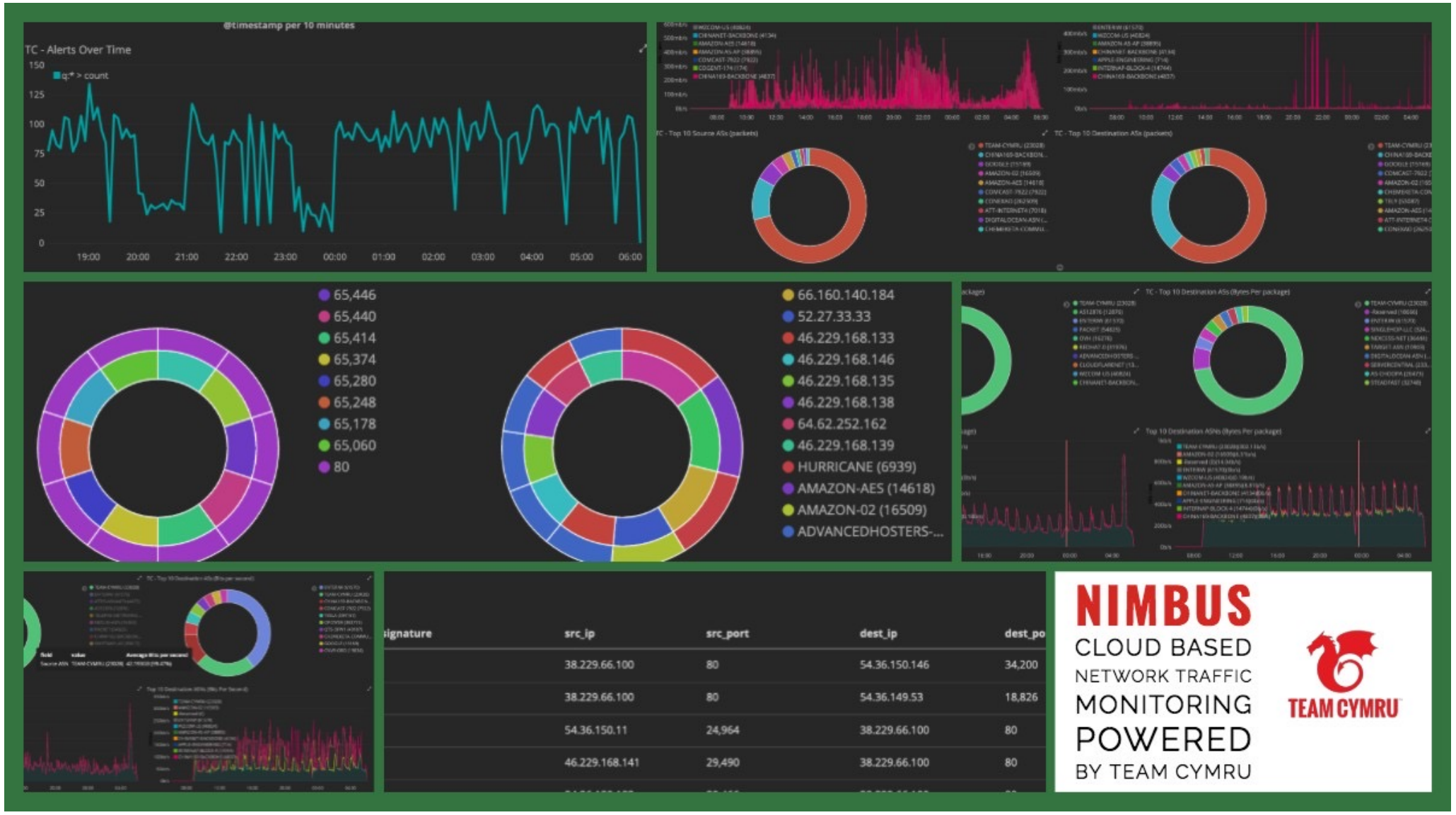
Use RPKI (Resource Public Key Infrastructure)

- Similar to ROAs, but block requests?
  (Signed message is the block request)

- “Discard Origin Authorizations” (DOA)?
  (Signed message delegates authority for block requests to another – UTRS)

What else? Your input and community input, please!

Nimbus Threat Monitor



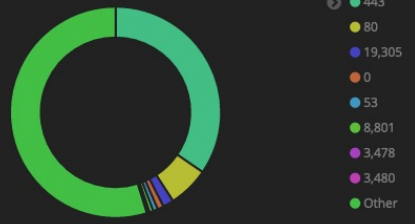
[TC - Alert] Alert Counts (numbers)

1.73 m

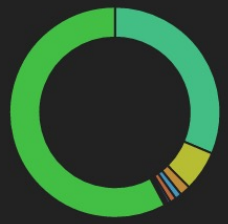
[TC - Alert] Top Protocols

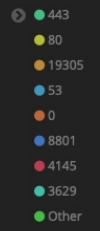
[TC - Alert] Top Channel

[TC - Alert] Top Source Ports

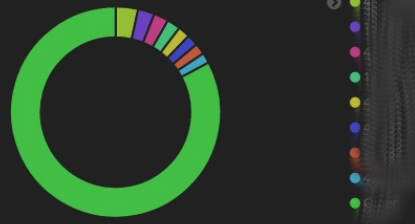


[TC - Alert] Top Destination Ports

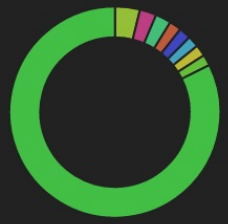




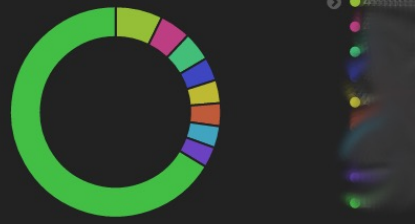
[TC - Alert] Top Source IP



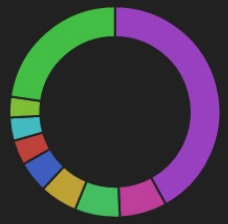
[TC - Alert] Top Destination IP



[TC - Alert] Top Alert IP



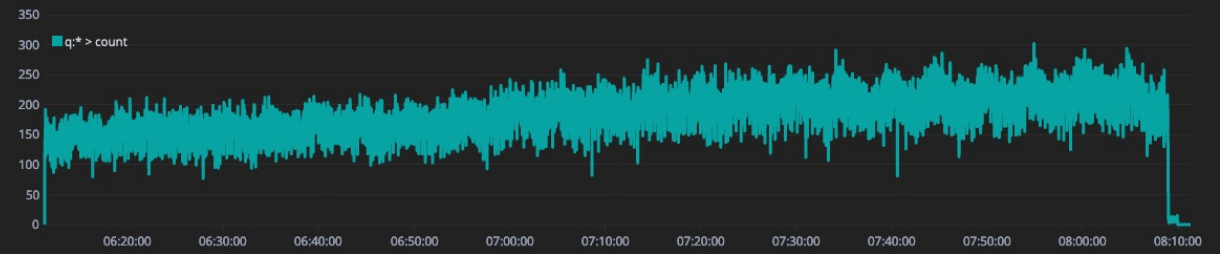
[TC - Alert] Top Alert ASNs



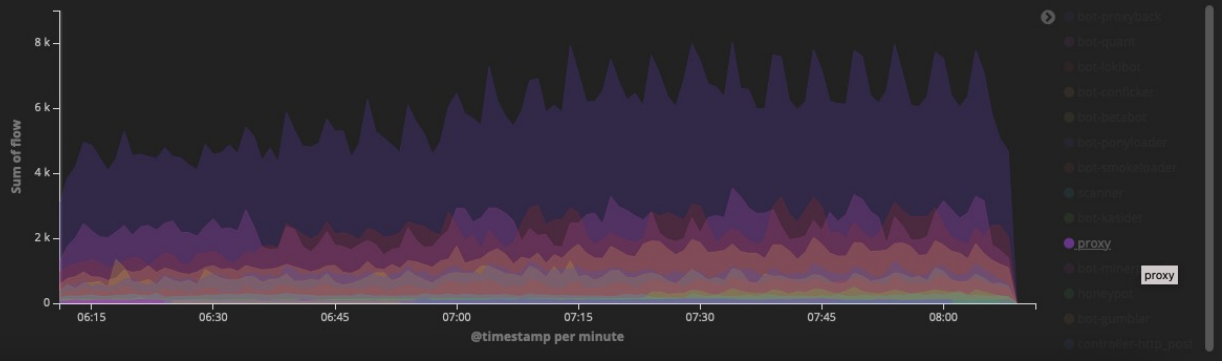
[TC - Alert] Top Signatures

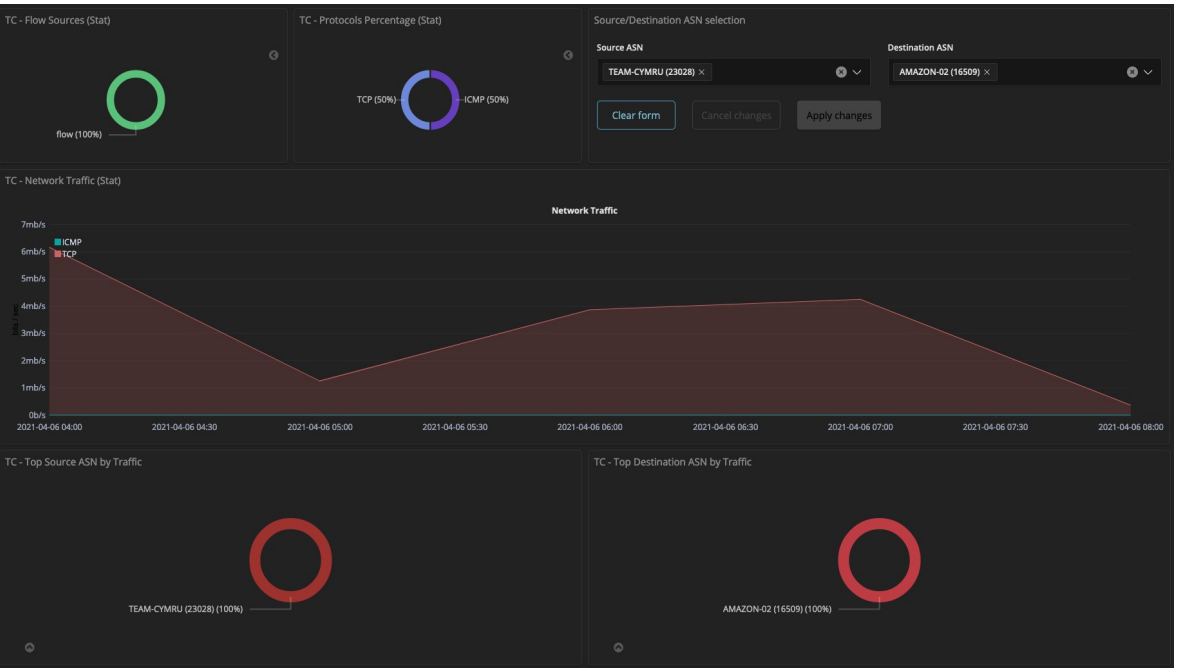
alert_signature: Descending	Sum of flow	Sum of bytes	Sum of pkts
bot-proxyback	691.558 k	1.395TB	2.142 b
bot-quant	274.825 k	542.458GB	804.376 m
bot-lokibot	249.326 k	588.384GB	770.454 m
bot-conficker	159.937 k	289.515GB	468.495 m
bot-ponyloader	107.159 k	194.36GB	307.276 m
bot-betabot	94.138 k	255.195GB	339.069 m
bot-smokeloader	63.572 k	98.679GB	173.904 m
scanner	27.882 k	2.195GB	29.31 m
bot-kasidet	19.144 k	59.799GB	72.156 m
proxy	10.526 k	2.444GB	10.923 m

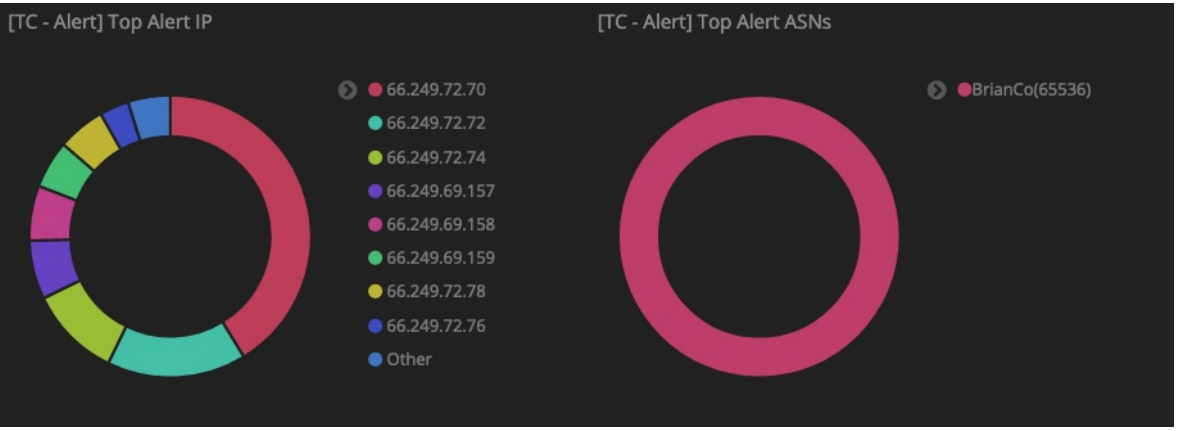
[TC - Alert] Alerts Over Time



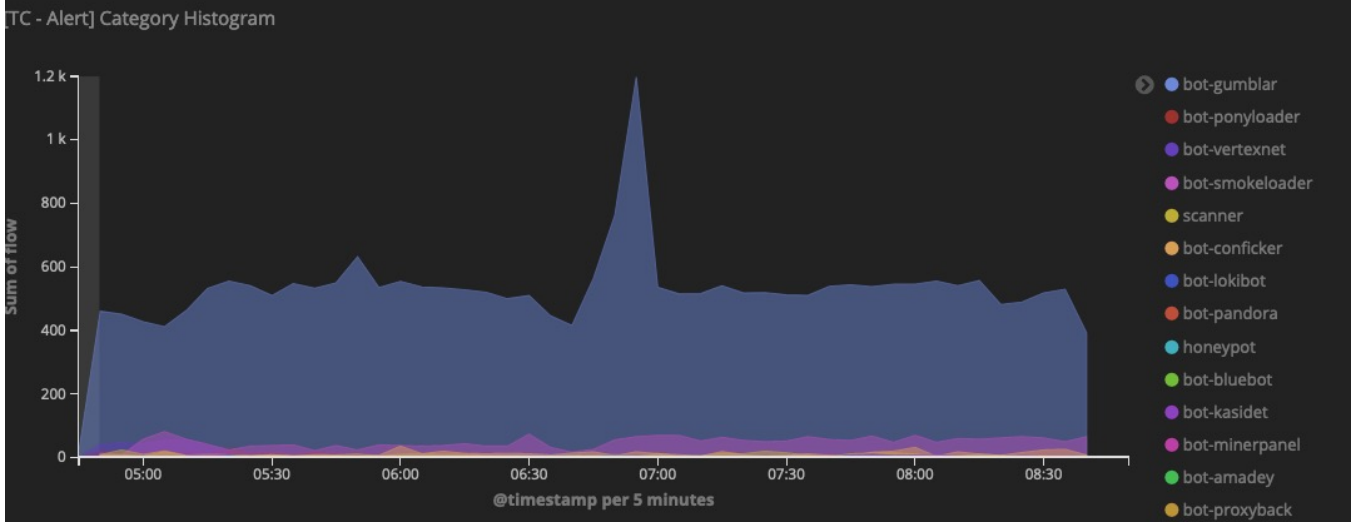
[TC - Alert] Category Histogram







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



Other Community Services

- Dragon News Bytes
- BOGON Reference Project
- IP to ASN Mapping
- Malware Hash Registry (MHR)
- CSIRT Assistance Program (CAP)

TEAM CYMRU™

Thank you

James Shank
jshank@cymru.com
outreach@cymru.com