TEAM CYMRU

Threat Intelligence with Community Services

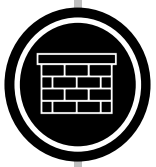
Brian Davenport

AGENDA

2:40 – 2:45 Who is Team Cymru?

2:45 – 2:55 Introduction to Metadata

2:55 – 3:00 NimbusTM



3:00 – 3:05 Community Driven DDOS Prevention

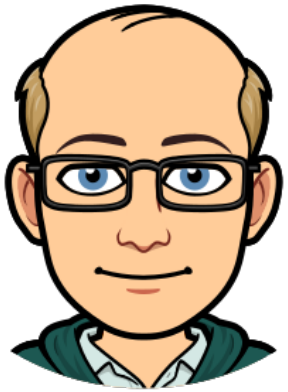
3:05 – 3:10 Question and Answer

About Me

Solutions Engineer

Dog Owner

Explorer

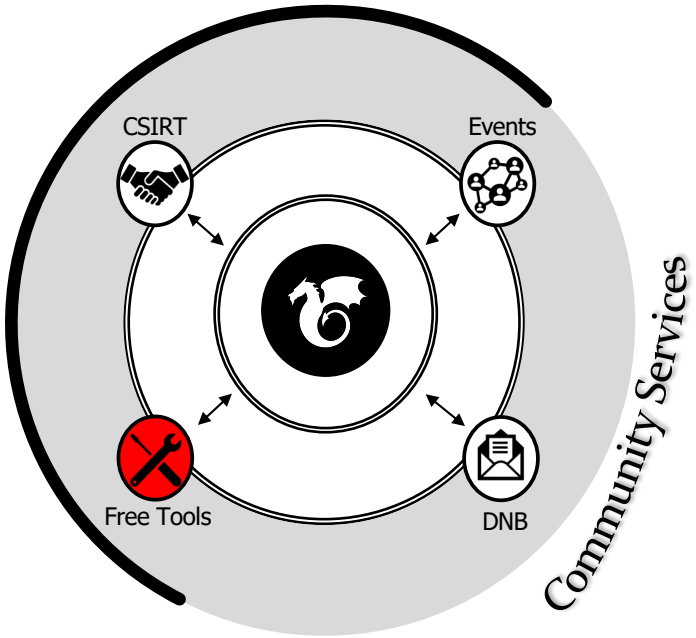


Technologist

Outreach Team

Mainer

Outreach



Free Tools

Solutions provided by Team Cymru

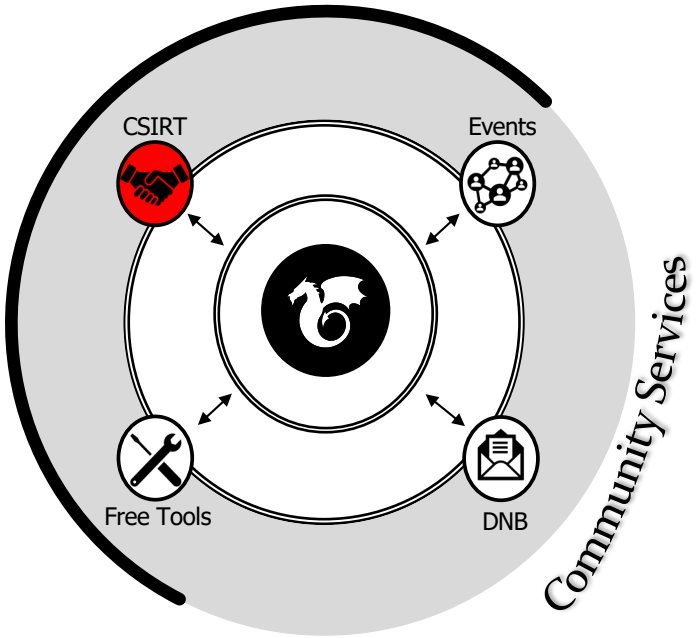
Nimbus Threat Monitor: Kibana-based appliance that integrates our insight about malicious activity on your network, with near real time alerting

Unwanted Traffic Removal Service (UTRS): A system that helps mitigate large infrastructure attacks by leveraging an existing network of cooperating BGP speakers such as ISPs, hosting providers and educational institutions that automatically distributes verified BGP-based filter rules from victim to cooperating networks.

IP To ASN Mapping Project: A query interfaces that allow for the mapping of IP addresses to BGP prefixes and Autonomous System Numbers (ASNs), based on BGP feeds from our 50+ BGP peers. Updated every 4 hours, this data is available through traditional WHOIS (TCP 43), DNS (UDP 53), HTTP (TCP 80), and HTTPS (TCP 443).

Malware Hash Registry (MHR): Similar to the Team Cymru IP address to ASN mapping project, the Malware Hash Registry (MHR) project is a look-up service with an added benefit: you can query our service for a computed MD5 or SHA-1 hash of a file and, if it is tracked malware, we return the last time we have seen it along with an approximate anti-virus detection percentage.

Outreach



CSIRT Assistance Program

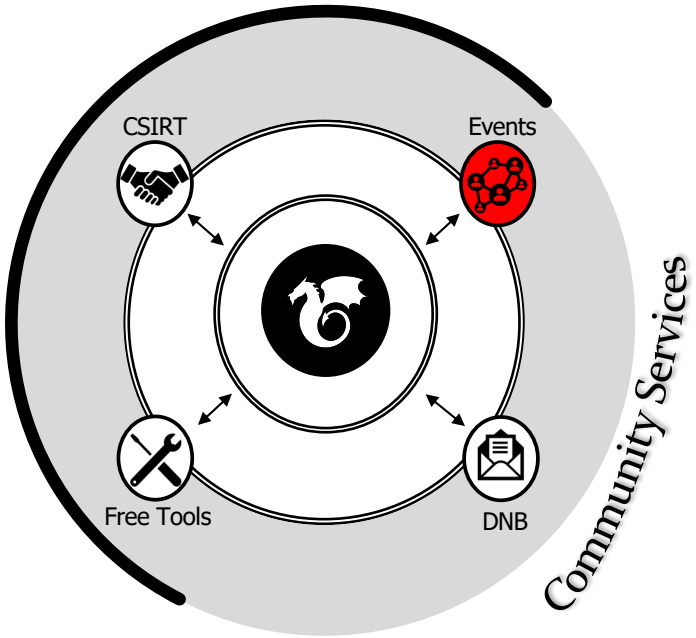
Free Threat Intel for Non-Commercial National and Regional CSIRT Teams.

Team Cymru works with national and regional CSIRT teams globally by sharing our world-class threat intelligence. We provide this unique Pure Signal™ intelligence at no cost to you. We want to help secure the Internet, and we want to keep you informed of what we see in your region

We provide intelligence on a variety of categories:

Bots / Controllers	Honeypot	Scanners
Brute-Force	Open Resolvers	Spam
Darknet	Phishing	Proxies

Outreach



Events

Team Cymru Conferences

We hold a series of Regional Information Security Events (RISE), as well as an annual conference called Underground Economy. These are exclusive events, centered on threat intelligence, cyber crime and cyber security issues, that include TLP-Amber and -Red case studies. In order to register for one of these events, please apply via the links below, and we will contact you with further instructions.

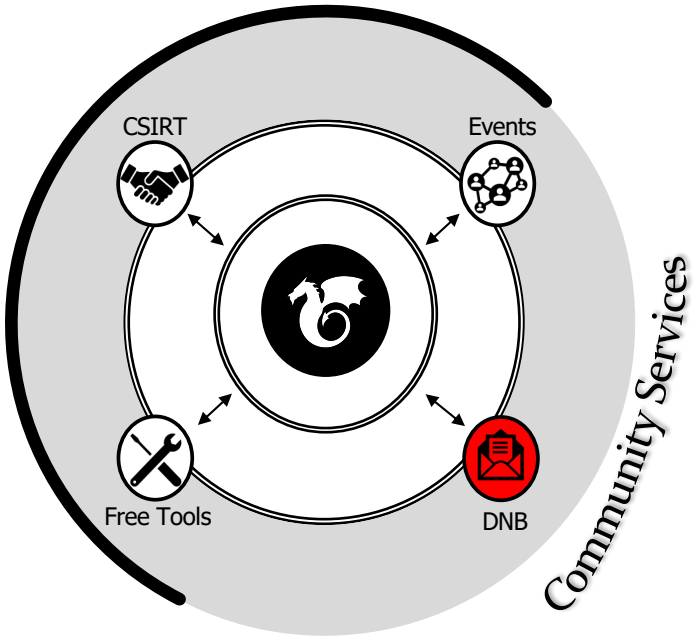
Team Cymru Webinars

We have a ongoing series called 'Dragons Den' where we talk with industry experts about current trends, participate in and sponsor regional events (e.g PacNOG), and host webinars around the globe to help keep communities up to date on what we are working on and seeing in the world of information security / intelligence.

Event Schedules

Visit our events page https://team-cymru.com/company/events/ follow us on Twitter @teamcymru and LinkedIn https://www.linkedin.com/company/team-cymru/

Outreach



Dragon News Bytes

Information Security News provided by Team Cymru

Dragon News Bytes is a private and restricted mailing list that distributes Information Security news articles. These articles may come from newspapers, magazines, and other online resources, as well as from Team Cymru's own research.

We will endeavor to tag the subject line with [DNB] and at least one other tag to suggest the topic:

[APT] – Advanced Persistent Threat, Nation State hacks and malware

[ARREST] – News of arrests, court matters and sentencing for InfoSec criminals

[ATTACK] – DDoS, defacements and criminal 'hacks'

[HACKTIVISM] – Anonymous, #OpAnything plus anything related to online protests

[MALWARE] – Viruses, botnets and other stuff we know you love

[MOBILE] – Anything related to Android, iOS Security

[POLICY] – Anything related to InfoSec policies, guidance and procedures

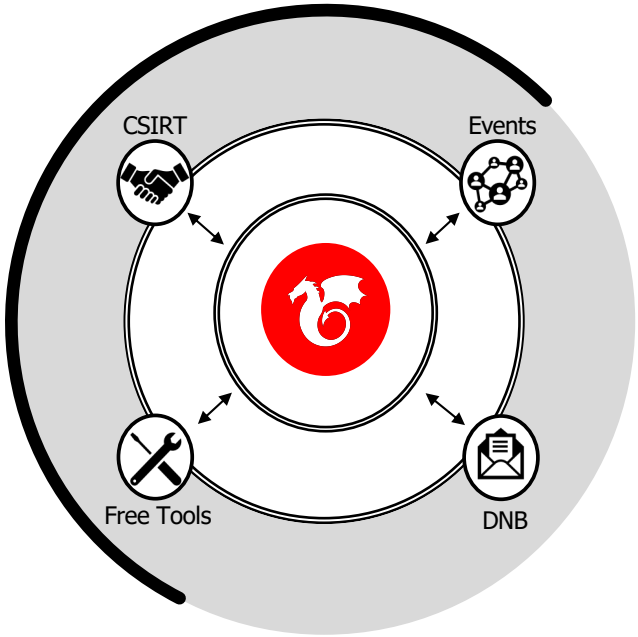
[PRIVACY] – Related to anything that impacts your personal privacy, OPSEC, data breaches, and information disclosures

[RESEARCH] – Papers and other new analysis and insight

[TIPS] – Anything else we can't categorize otherwise

[VULNS] – Anything related to vulnerabilities, patching, etc

Team Cymru



Who we Are

We uncover the who, what, when, where and why of malicious behavior.

15 years of service to network defenders, internet operators and cybercrime investigators worldwide.

- Free services for 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.

Team Cymru is comprised of former…

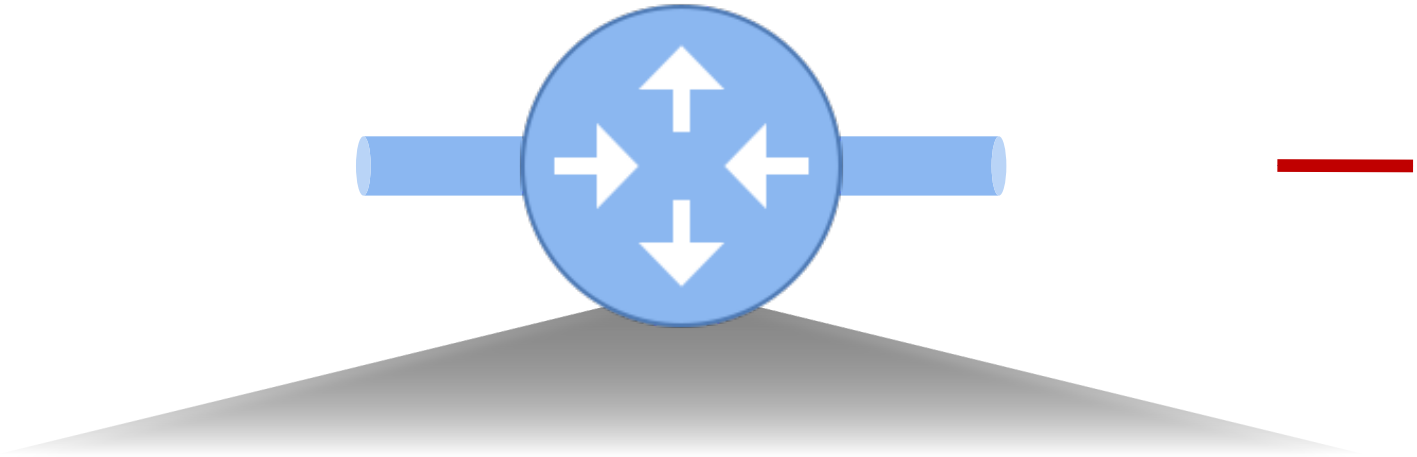
- Members of national and industry CSIRT teams
- Law enforcement
- Analysts from research, education, private and public sectors
- ISP backbone engineers
- Fortune 500 enterprise network engineers
- Penetration testers
- Military – US and allied nations
- Frontend, backend, gaming, web app, kernel, high-performance computing and big data developers and system engineers

Using Metadata for Threat Intelligence

- Maximize existing investment in network equipment by using built in protocols.
- Passive Monitoring – no need to install agents or expensive probes.
- If something happens on the network, flow data will see it.
- Enriching metadata with additional detail extends use cases and increases value.
- Wide support from a variety of vendors.

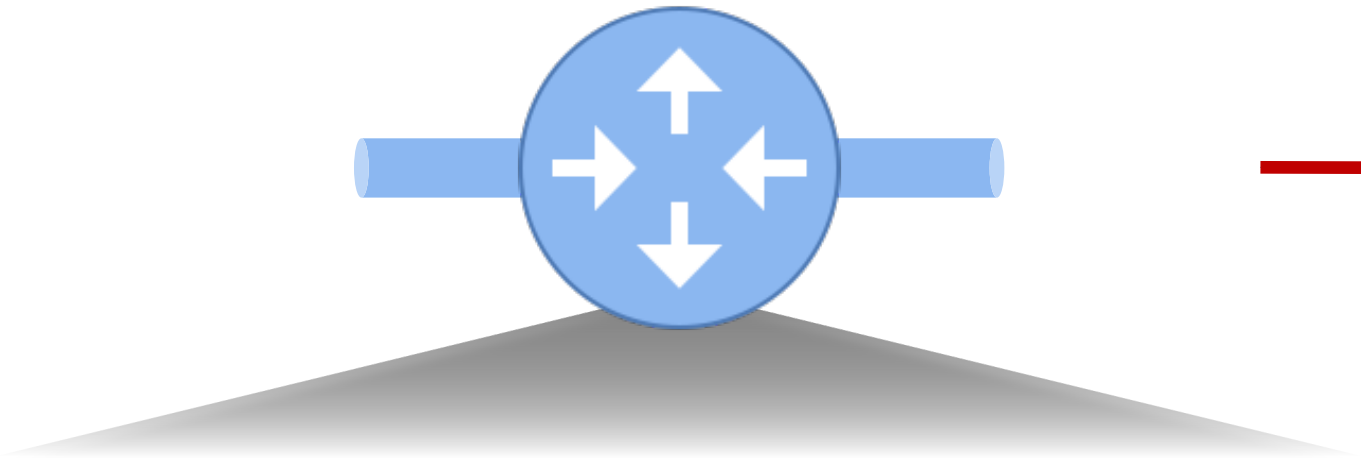
Flow Data – How it works…

TEAM CYMRU



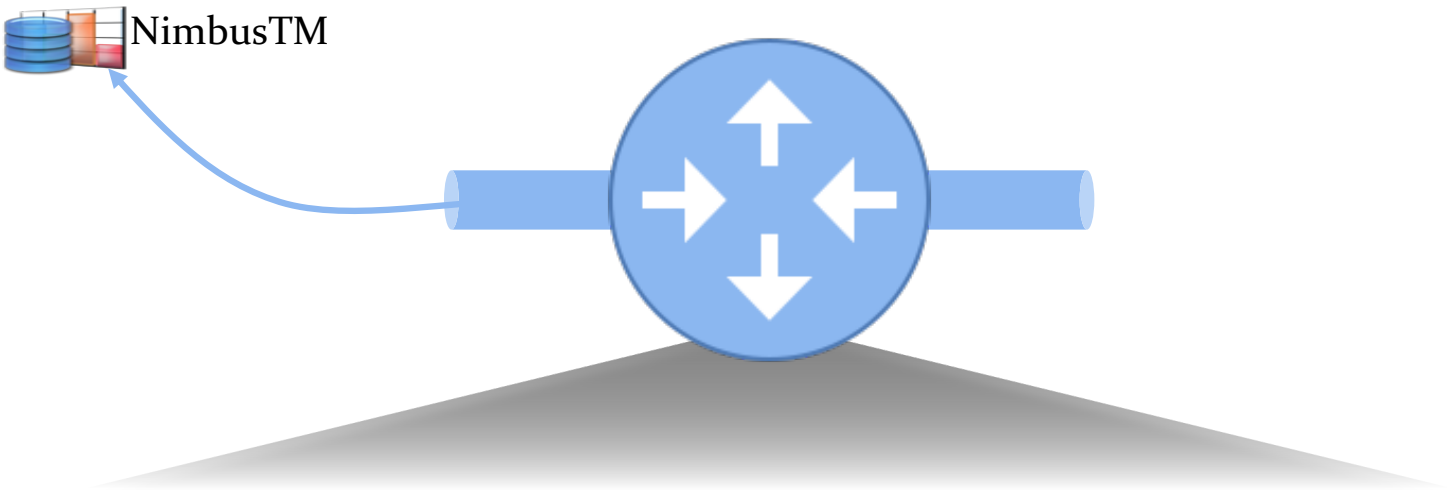
Destination IP	Source IP	Destination Port	Source port	Source Interface	Protocol	Bytes
8.8.8.8	1.1.1.1	80	65000	1	TCP	100

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	600
4.4.4.4	2.2.2.2	80	64500	1	TCP	50

TEAM CYMRU

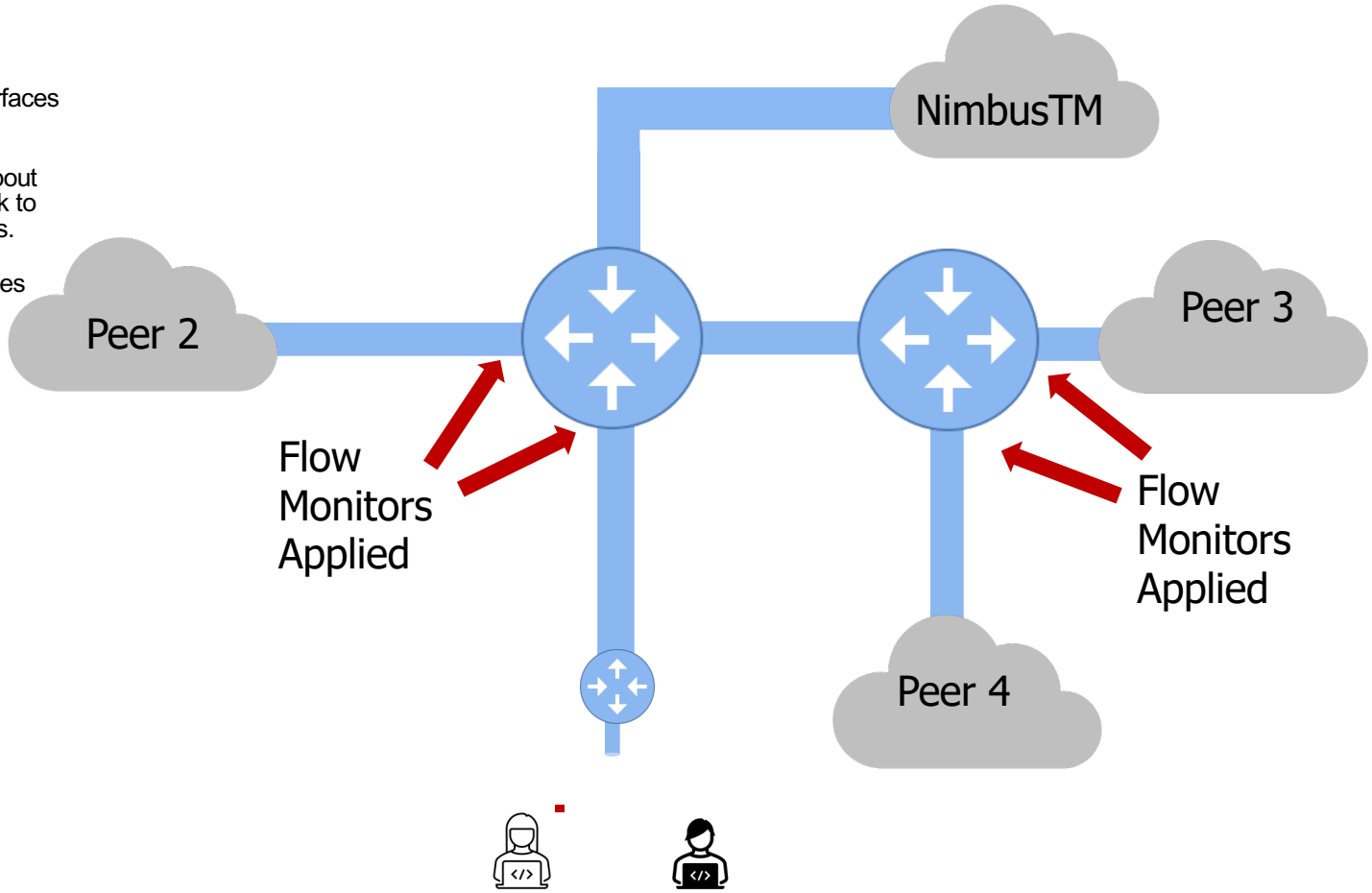


Destination IP	Source IP	Destination Port	Source port	Source Interface	Protocol	Bytes
8.8.8.8	1.1.1.1	80	65000	1	TCP	600
4.4.4.4	2.2.2.2	80	64500	1	TCP	50

Where to gather data from?

TEAM CYMRU

- 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.



NimbusTM

- Cloud based collector, built on Elastic / Kibana.
- Free to use for ISPs, hosting providers, 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.

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	BrianCo (65536)	Brian Malware	100


TC - Flow Sources (Stat)
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
Destination ASN
[TC - Alert] Alert Counts (numbers)
1.73 m
[TC - Alert] Top Protocols
UDP (26.27%)
TCP (72.84%)
[TC - Alert] Top Channel
router_01 (36.52%)
router_02 (63.48%)
[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] Top Source Ports
443
80
19,305
0
53
8,801
3,478
3,480
Other
[TC - Alert] Top Destination Ports
443
80
19305
53
0
8801
4145
3629
Other
[TC - Alert] Alerts Over Time
q:* > count
350
300
250
200
150
100
50
0
06:20:00
06:30:00
06:40:00
06:50:00
07:00:00
07:10:00
07:20:00
07:30:00
07:40:00
07:50:00
08:00:00
08:10:00
[TC - Alert] Top Source IP
[TC - Alert] Top Destination IP
[TC - Alert] Category Histogram
8 k
6 k
4 k
2 k
0
Sum of flow
06:15
06:30
06:45
07:00
07:15
07:30
07:45
08:00
@timestamp per minute
proxy
proxy
[TC - Alert] Top Alert IP
[TC - Alert] Top Alert ASNs
0
05:00
05:30
06:00
06:30
07:00
07:30
08:00
08:30
@timestamp per 5 minutes
bot-kasidet
bot-minerpanel
bot-amadey
bot-proxyback

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

TEAM CYMRU

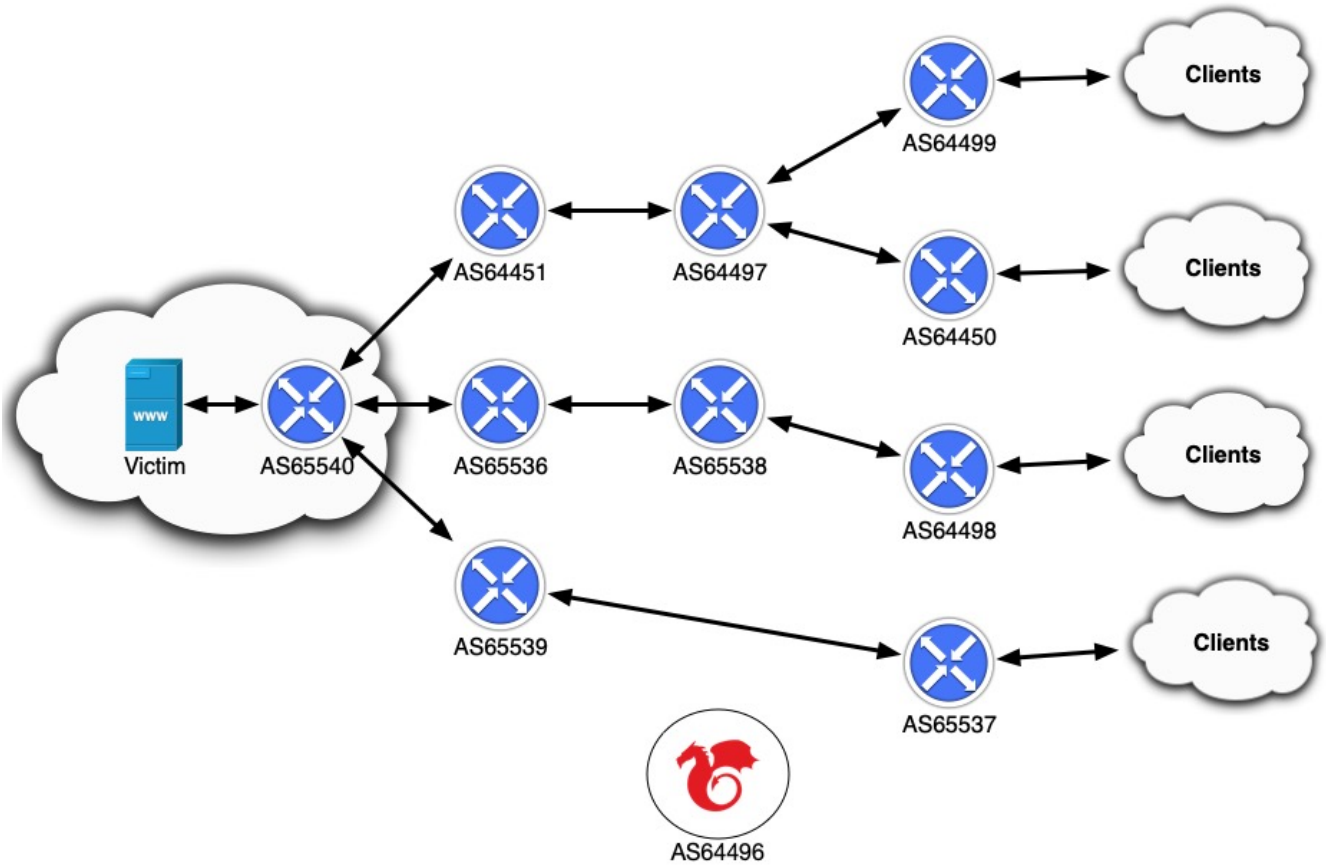
BGP based triggers, with two basic rules:

- 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)

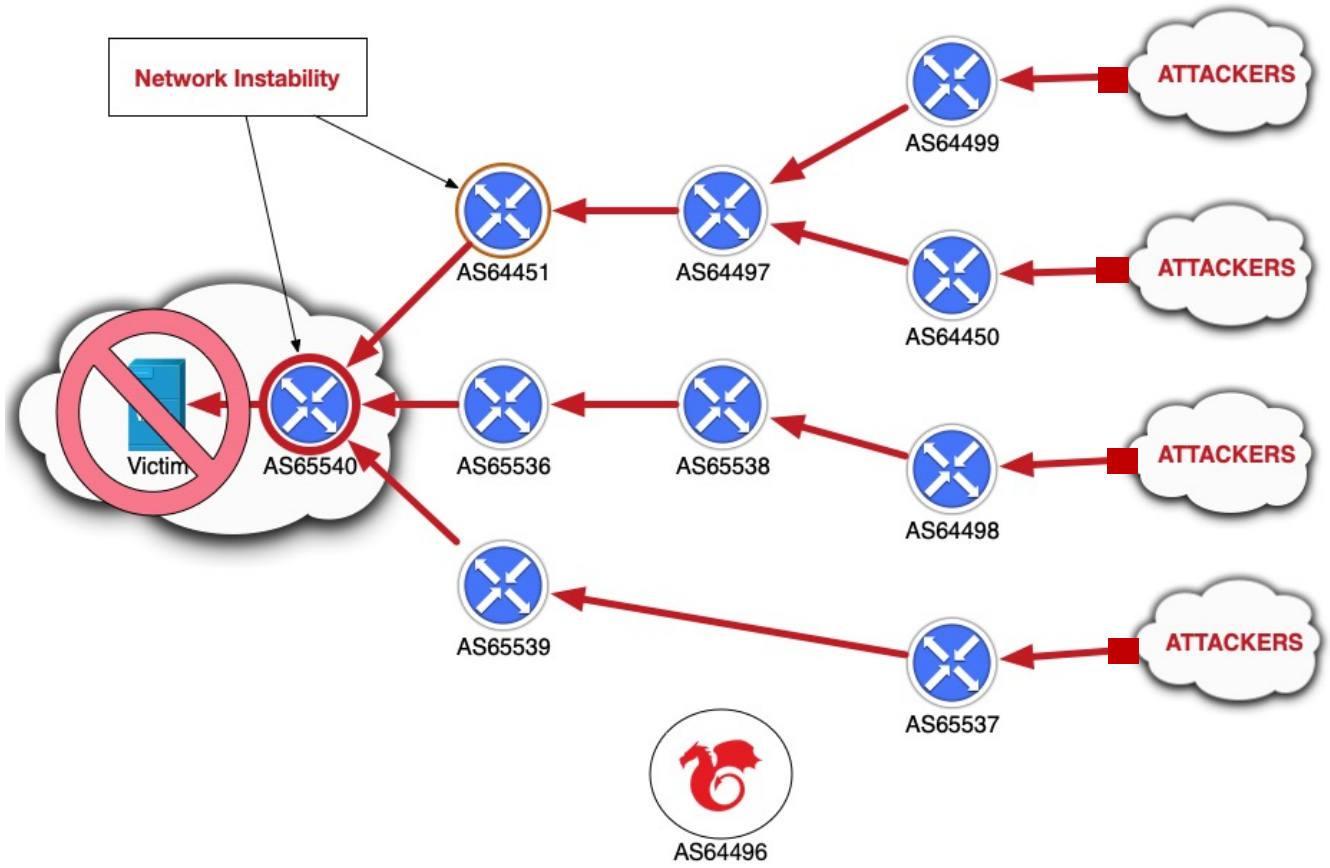
UTRS

TEAM CYMRU



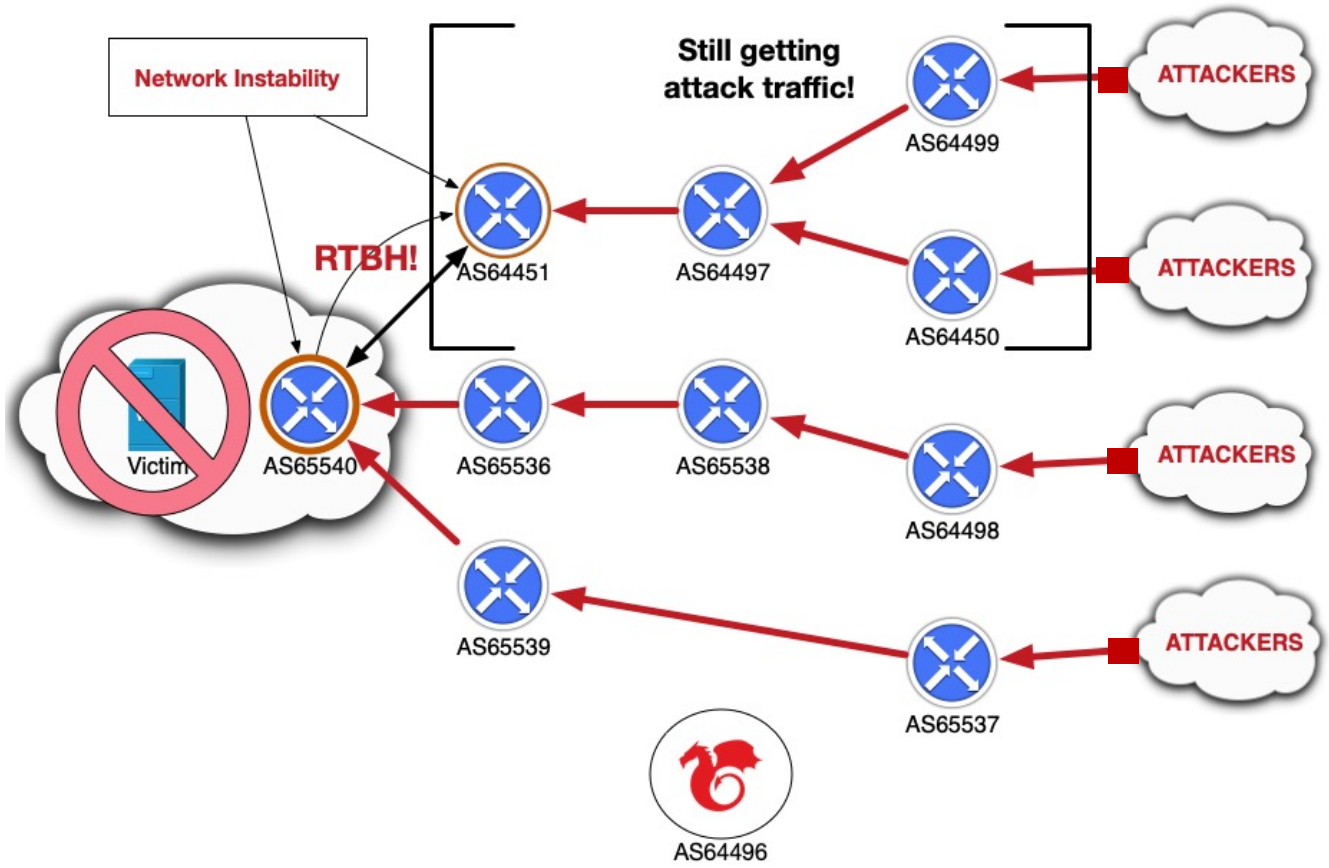
UTRS

TEAM CYMRU



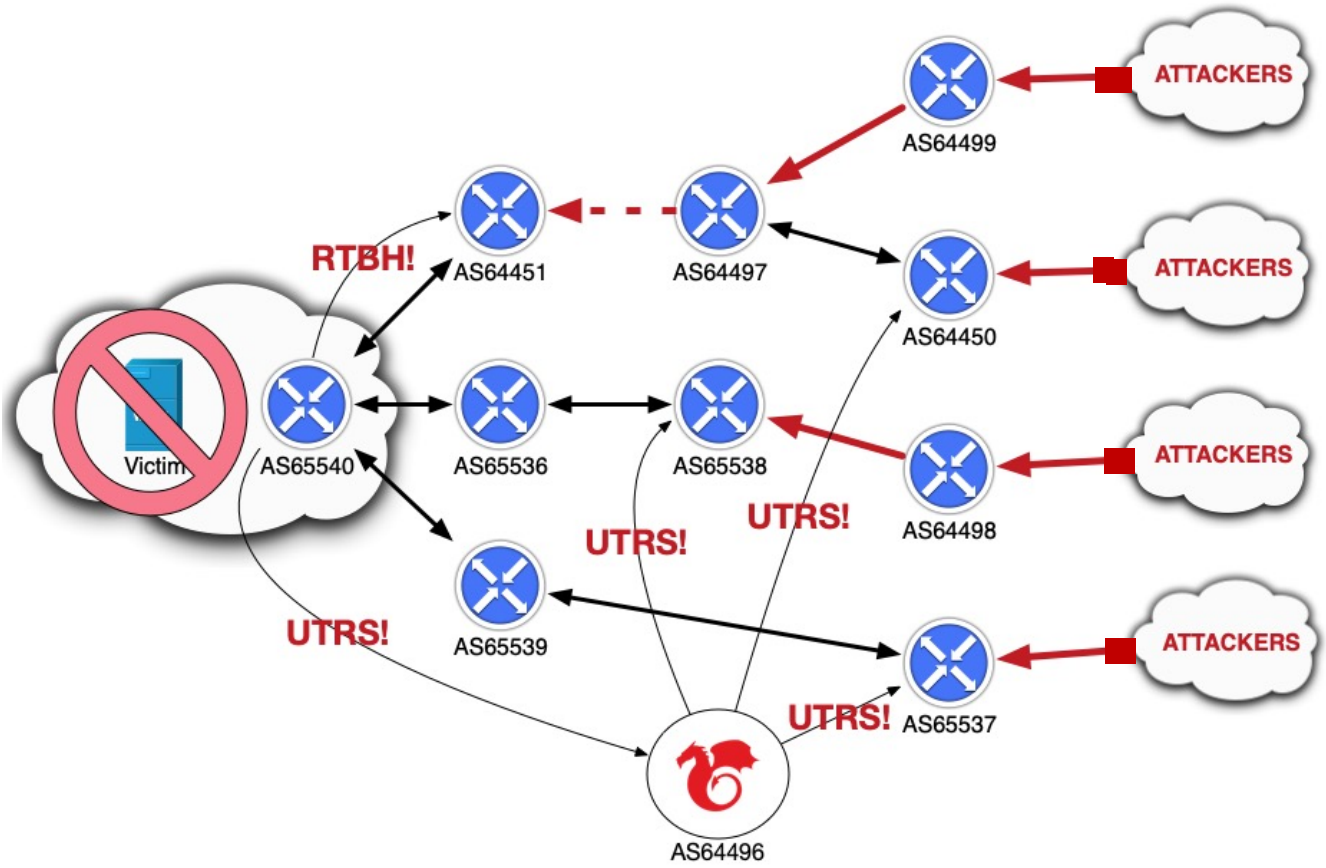
UTRS

TEAM CYMRU



UTRS

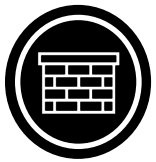
TEAM CYMRU



Thank you!

Become a Nimbus Partner

https://team-cymru.com/community-services/nimbus-threat-monitor/



Join our Community DDOS Mitigation Project

https://team-cymru.com/community-services/utrs/

Connect with Team Cymru on Social Media

@teamcymru

Connect with Brian Davenport on LinkedIn

https://www.linkedin.com/in/briandavenport1/