TEAM CYMRU

Why IX's matter for Enterprise Security and Reliability

John Brown, CISSP, CP-AMEL

Security Classification / Pictures of Slides

TEAM CYMRU

- This presentation is marked as TLP:CLEAR
- What is TLP (Traffic Light Protocol) ?
- See https://www.first.org/tlp/
- Taking pictures of slides is PERMITTED
- Please try to keep other peoples faces out of the pictures
- The entire presentation will be available via email, just ask me

AGENDA

Introduction / Who am I?

Review on Transit vs Peering

What are Exchange Points / IX's

So Why Peer? / Benefits of Peering

Peering Importance to NetOps / SecOps

Questions and Answers

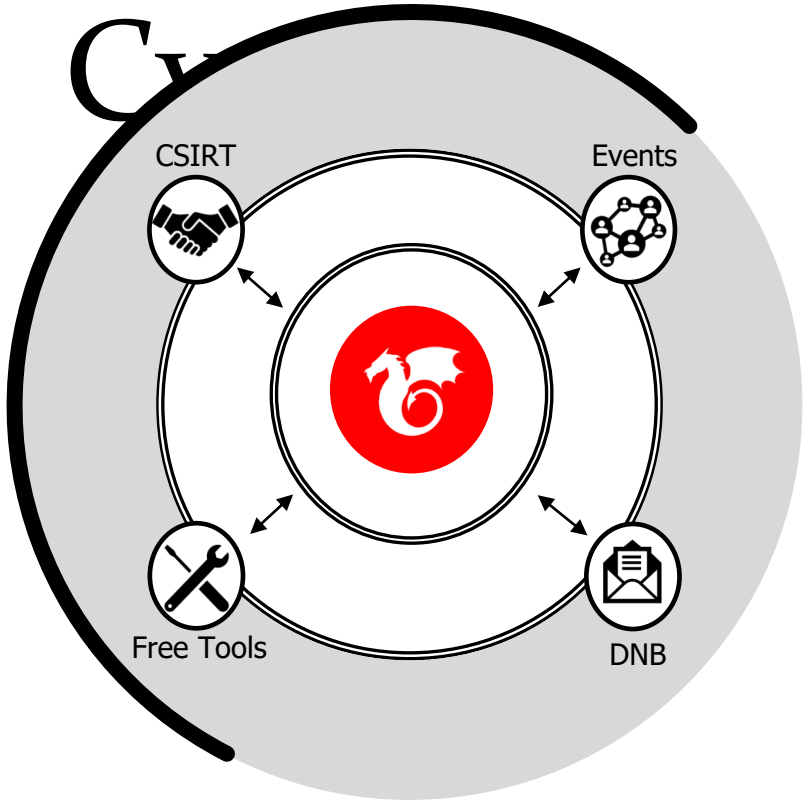
About Me

TEAM CYMRU

- John Brown, CISSP, CP-AMEL
- Senior Security Evangelist at Team Cymru
- 35+ years as software and network engineer
- Have built Internet networks on 3 continents
- Past owner of a regional ISP business (fiber / wireless)
- Passionate about helping ISP's improve their network security
- Past Mikrotik Authorized Instructor (MT-CNA, MT-CRE, MT-CINE)
- Ran ICANN's L-ROOT DNS Server, one of 13 critical DNS servers
- Commercial Multi-Engine Airplane Pilot
- When not working, I enjoy flying airplanes.

I can be reached at: jbrown+netnod23@cymru.com

Team Cy



Who we Are

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

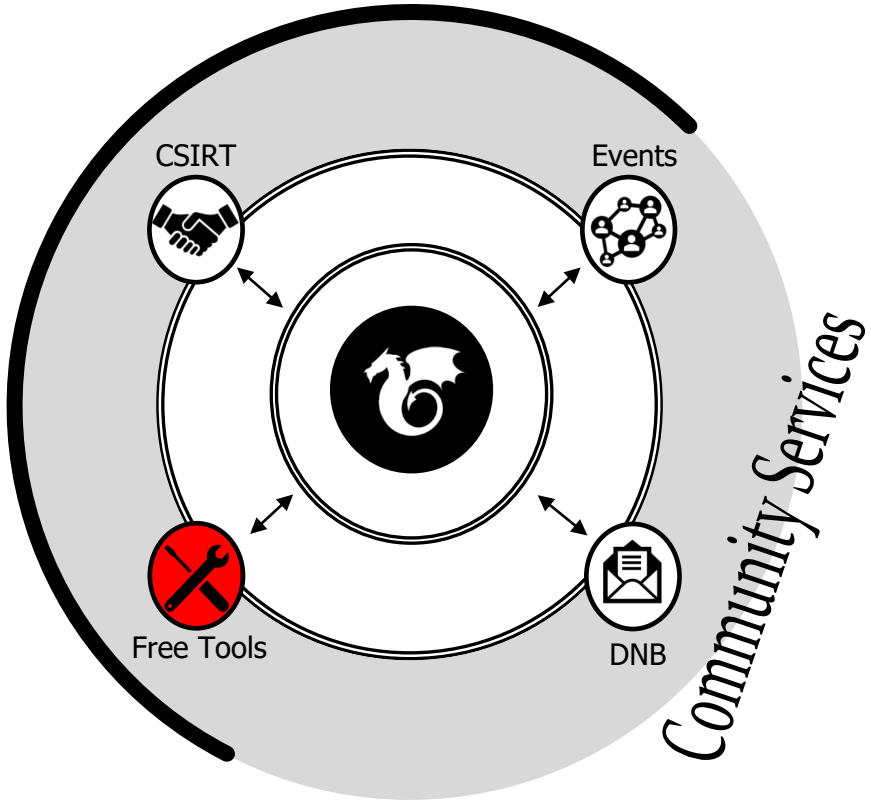
15+ years of service to network defenders, internet operators and cybercrime investigators worldwide.

- No Cost Services for ISPs, hosting providers and CSIRTs
- Unmatched eco-system of trusted data sharing and collaboration partnerships worldwide
- Work with 140+ CSIRT teams in 86+ countries
- Relied on by many security vendors, Fortune 100 companies, and public sector teams.

TLP:CLEAR

Outreach

No-Cost Community Tools



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

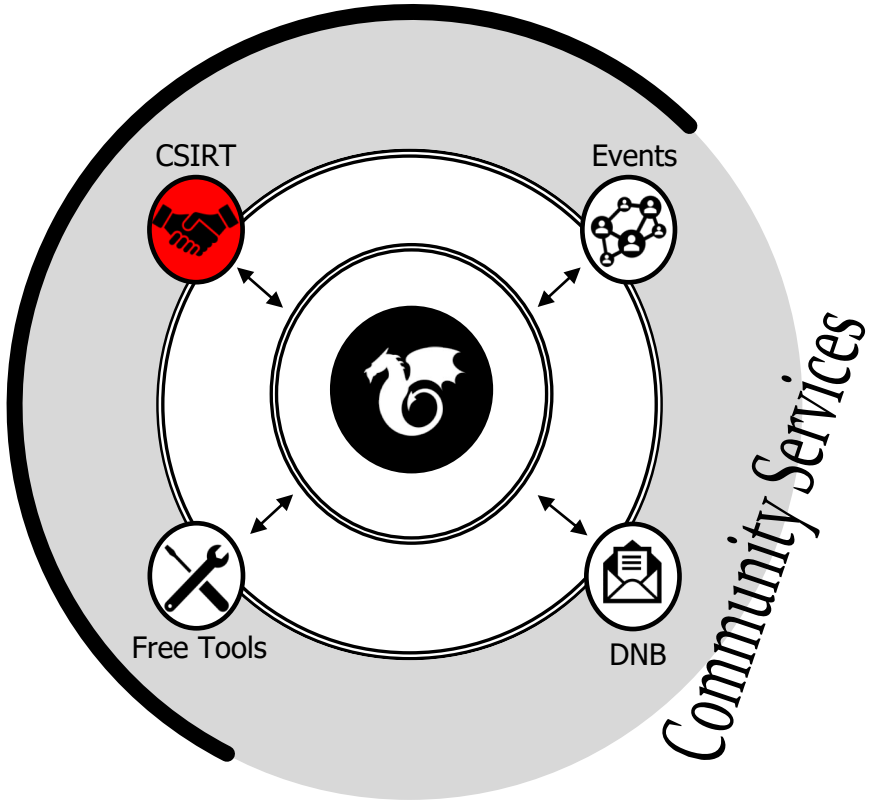
Community Based DDOS Mitigation: A system that helps mitigate large infrastructure attacks by leveraging an existing network of cooperating BGP speakers such as ISPs, hosting providers, educational institutions and enterprise networks that automatically distributes verified BGP-based filter rules from victim to cooperating networks.

BOGON'S Routing Information: BOGONS are network prefixes that should never appear in the public Internet routing table. These include Private IP blocks, Unallocated, Reserved, Special addresses, and blocks not currently allocated by a RIR. This information is provided via BGP, TXT, HTML feeds.

More Info: https://www.team-cymru.com/community-services

TLP:CLEAR

Outreach



CSIRT Assistance Program

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

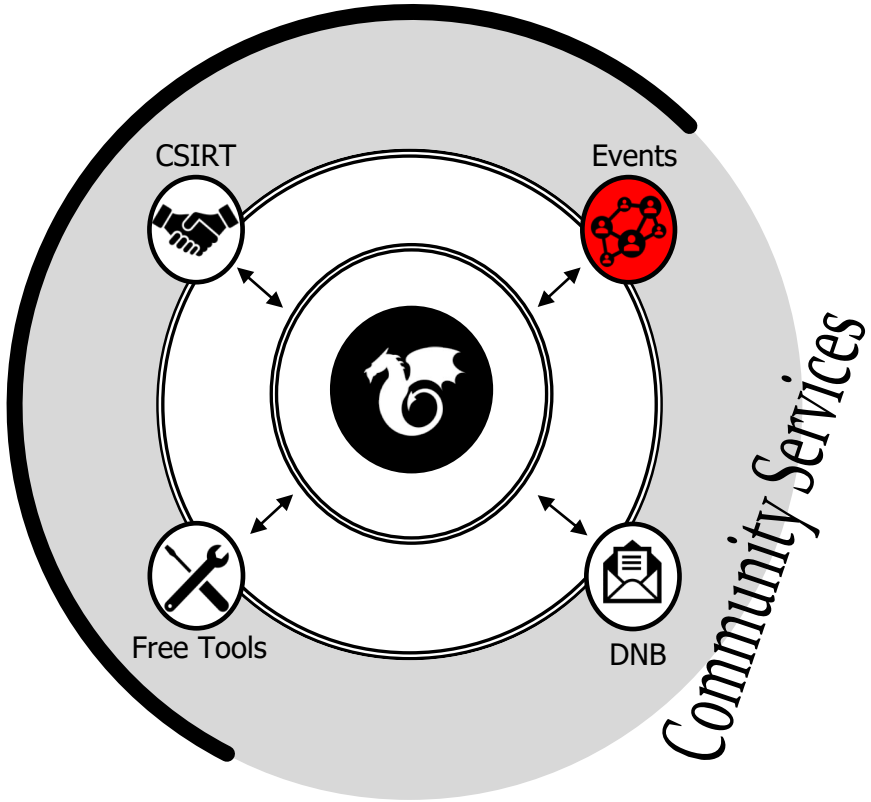
Team Cymru works with national and regional CSIRT teams globally by sharing our world-class threat intelligence. We provide this unique Pure Signal™ intelligence at no cost to you. We want to help secure the Internet, and we want to keep you informed of what we see in your region

We provide intelligence on a variety of categories:

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

TLP:CLEAR

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

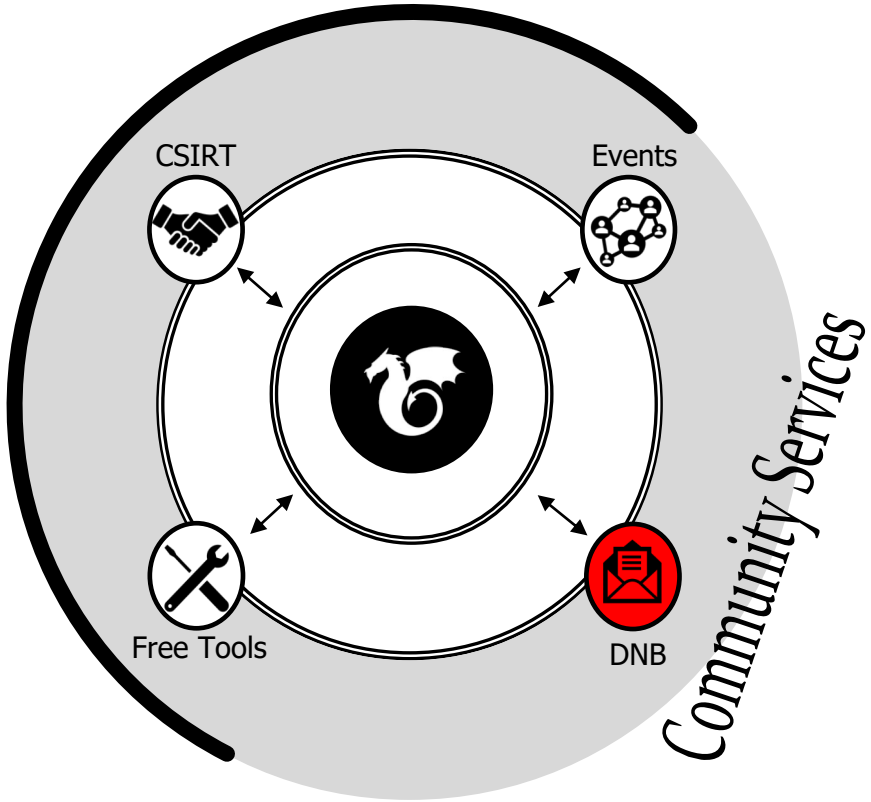
We have a ongoing series called 'Dragons Den' where we talk with industry experts about current trends, participate in and sponsor regional events (e.g PacNOG), and host webinars around the globe to help keep communities up to date on what we are working on and seeing in the world of information security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

Event Schedules

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

TLP:CLEAR

Outreach



Dragon News Bytes

Curated 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.

TLP:CLEAR

AGENDA




Introduction / Who am I?

Review on Transit vs Peering

What are Exchange Points / IX's

So Why Peer? / Benefits of Peering

Peering Importance to NetOps / SecOps

Questions and Answers

Review Transit vs Peering

TEAM CYMRU

- What is Transit
  - Transit is the paid service by which you pay your ISP to connect you to the entire global internet.
  - Your ISP has the responsibility of carrying your packets to / from the global internet. How they do that is left up to them.
  - Smaller ISP's will generally purchase Transit from larger ISP's
  - Enterprise networks typically just purchase Transit from one or more ISP's. (Spoiler Alert, we hope to break this somewhat in this talk ☺️)

Review Transit vs Peering

TEAM CYMRU

- What is Peering
  - Peering is the direct interconnection between two networks.
  - Sometimes this is settlement free (no cost), sometimes there is a fee.
  - You are exchanging YOUR routing information with the peer, and they are exchanging their direct routing information with you.
  - There is ZERO expectation that either peer (neighbor) can get packets to the global internet. This is only a network to network connection.
  - ISP's typically exchange their routes and their customer routes with peers

TLP:CLEAR

Review Transit vs Peering

TEAM CYMRU

- What is Peering
  - Peering requires BGP (Border Gateway Protocol) to be used between the peers.
  - BGP is used to communicate the peers routing information.
  - Peering is typically established by building a direct network connection between the peers. (Some scaling issues here.)

AGENDA

Introduction / Who am I?

Review on Transit vs Peering

What are Exchange Points / IX's

So Why Peer? / Benefits of Peering

Peering Importance to NetOps / SecOps

Questions and Answers

What are Exchange Points / IX's

- Internet Exchanges solve a scaling problem
  - Remember that to establish a peering session you need to connect the two networks. This is sometimes via a private line / leased circuit.
  - If you have dozens or hundreds of peers, that potentially means lots of private line circuits. This is cost prohibitive and doesn't scale well.
  - An Internet Exchange, or Exchange Point provides a facility to allow interconnection of peers at a much lower cost and at scale.
  - Typically, IXP's have equipment at Data Centers that enable peers to interconnect. Generally, this is via ethernet technologies.
  - The more peers at an IX, the better it can attract even more peers…..

AGENDA

Introduction / Who am I?

Review on Transit vs Peering

What are Exchange Points / IX's

So Why Peer? / Benefits of Peering

Peering Importance to NetOps / SecOps

Questions and Answers

So why peer ?

TEAM CYMRU

- Peering does the following:
  - Reduces latency between the neighbors
  - Improves customer experience
  - Reduces network costs
  - Improves reliability / network resiliency
  - If 20% of your traffic is from Netflix, then having a direct link with Netflix is a smart thing for both you and Netflix.
  - Keeps “in region” traffic ”in region”. No need to send packets to London if they are only going to Malmö .

So how does peering work ?

TEAM CYMRU

- With peering you exchange local routing information
  - This means YOUR router now has a direct link to your peers network
  - All packets going from your network to the peers network will now go across this direct link.
  - This traffic will NOT go across your Transit connection
  - This improves reliability, performance, reduces latency, enhances Customer Experience.

AGENDA

Introduction / Who am I?

Review on Transit vs Peering

What are Exchange Points / IX's

So Why Peer? / Benefits of Peering

Peering Importance to NetOps / SecOps

Questions and Answers

Enterprise Peering NetOps / SecOps

TEAM CYMRU

- Peering should be an important part of your network and security design.
  - Typically, Enterprises (Banks, Government, Military, Schools, Legal, Accounting, etc.) typically only look at Transit. Their IT departments go out and buy transit from ISP(s). This is the way it's always been done! 😐
  - When there is a network problem, it's the ISP's issue.
  - If you have a DDOS (Distributed Denial Of Service, a form of attack), then the Transit ISP is the one to "deal with it", but your network is still down.
  - If you have a Fiber Cut, your Transit may be down, but Peering maybe UP

TLP:CLEAR

Enterprise Peering NetOps

TEAM CYMRU

- Peering in Network Operations (NetOps) is more than just pushing packets.
  - BRAND PROTECTION / ENHANCEMENT.
  - CUSTOMER EXPERIENCE. (better experience, happier customers)
  - RESILIENCE / RELIABILITY.
    - Fiber cuts, Transit Vendor Outage, H/W Fail
  - OPEX (COST) REDUCTION.
    - Bandwidth across peers is lower cost
    - Better Cloud Provider interconnection, can save up to 30%
  - TRAFFIC REDIRECT / ISOLATION / INVESTIGATION

- Peering is a Strategic Business Decision that impacts the entire org.

Enterprise Peering SecOps

TEAM CYMRU

- Peering in Security Operations (SecOps) is more than just protection.
  - BRAND PROTECTION / ENHANCEMENT.
  - CUSTOMER EXPERIENCE. (better experience, happier customers)
  - RESILIENCE / RELIABILITY
    - Routing Hijacks less likely of an impact, Better partner traffic flows
    - Risk Management, spread your connectivity risks out over many peers
    - DDOS Attacks are potentially able to be better mitigated

- Peering is a Strategic Business Decision that impacts / improves the entire org.

TEAM CYMRU

DDOS Attack

TLP:CLEAR

NEWS

Teenager suspected of crippling Dutch banks with DDoS attacks

A large distributed denial of service attack on banks and other organisations in the Netherlands, first thought to emanate from Russia, is now thought to have been launched by a local teenager

By **Tijs Hofmans**

Published: **08 Feb 2018 9:09**

What happened, how peering could have helped

- The attacker purchased a stressor service (DDOS for Hire) for around 650 SEK per week.
- The service crippled multiple Dutch banks for around a week.
- These Banks were not connected to Exchange Points.
- All of the DDOS traffic came across their Transit links.
- Customers could not access their bank account via online apps!

What happened, how peering could have helped

- Within the Netherlands is one of the Largest IX's in the world. AMS-IX.
- Based on information in PeeringDB.COM and AMS-IX website
  - None of the Banks were connected to an IX, including AMS-IX

- Had the Banks been connected to an IX such as AMS-IX, then the impact of the attack would have been very different.
- Local Dutch customers connected to ISP's connected to AMS-IX would have seen their packets go to/from the banks across the peering connections.
- DDOS impact would have been much less.

TLP:CLEAR

Other Examples

TEAM CYMRU

- Fiber Cut, Transit provider is now down. All your eggs are in a one basket
  - With Peering, you won't get to the entire Internet
  - BUT you will have a good chance of still getting to Local customers
- Regional Conflict
  - Your country or region is cut off for various reasons
  - Your LOCAL IX will still have the ability to connect you to in-region customers.
- The word CUSTOMER can be replaced with Business Partner / Vendor

What steps should Enterprises take to Peer?

TEAM CYMRU

- Apply with Regional Internet Registry for an ASN, if you don't have one
- Research PeeringDB.com https://www.peeringdb.com/ to learn what exchanges are in your area of operations
- Attend one or more Peering Forums ☺️
- Make sure your routing equipment can handle the requirements
- Get a connection to the local peering fabric and establish a session
- Register yourself into PeeringDB.
- Start peering with other local networks. Some of this will be easy, MLPA

What steps should IX's take ?

- Work to create educational outreach to critical enterprise organizations
- Create content that helps Enterprises understand peering, tools, equipment
- Invite Enterprise orgs to Peering Forums, like NetNod
- Work with existing members to characterize traffic to/from key enterprises
- Build an economic case on why Enterprises should peer at your IX!
- Help Register them into PeeringDB and similar tools, IRR's
- Help with RPKI / ROA as needed

Security Considerations

TEAM CYMRU

- You may need to adjust how your network firewall(s) interact with the new peering connections.
- Understand how you will announce routes to Peers vs Transit
  - You might want more specific via Exchange and aggregate via Transit.
- Make sure your RIR records are up to date.
- Create RPKI / ROA records for your prefixes.

The Ask

TEAM CYMRU

Lets work together on getting critical Enterprises connected to your IX

AGENDA

Introduction / Who am I?

Review on Transit vs Peering

What are Exchange Points / IX's

So Why Peer? / Benefits of Peering

Peering Importance to NetOps / SecOps

Questions and Answers

Thank You!

Questions ?

Me: John Brown, jbrown+netnod23@cymru.com

References

Team Cymru: https://www.cymru.com

Peeringdb: https://www.peeringdb.com/

First Org: https://www.first.org/tlp/