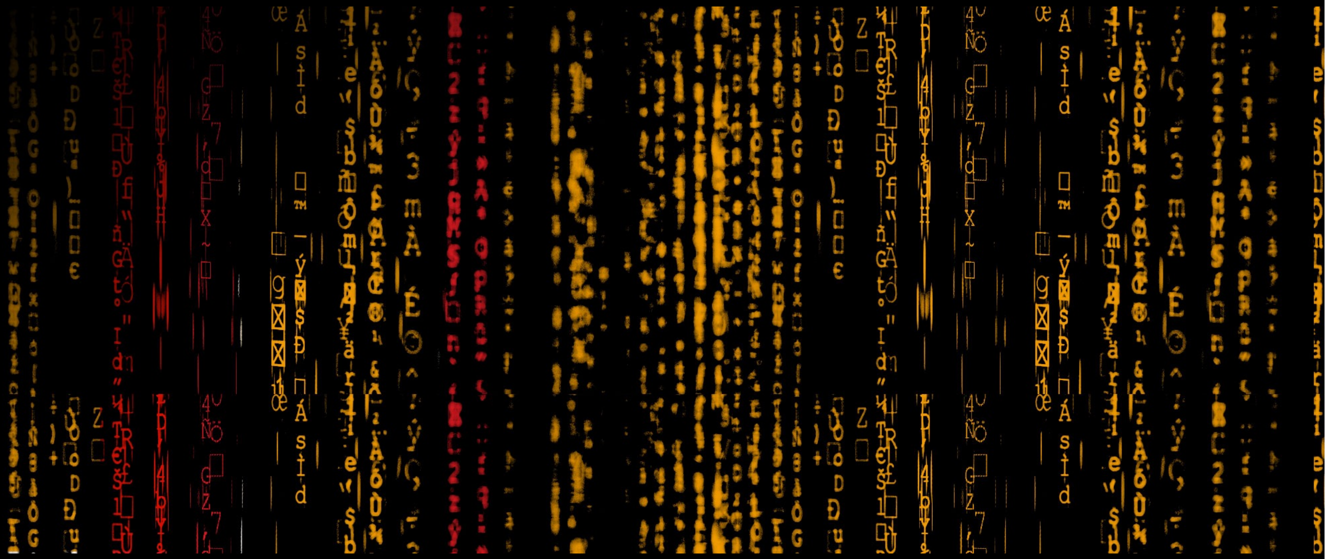
TEAM CYMRU

Network Hygiene
Let's clean up the network
Peering and IX’s



John Brown, CISSP, CP-AMEL, Team Cymru

Trademark Disclaimer

All trademarks, logos and brand names are the property of their respective owners. All company, product and service names used in this website are for identification purposes only. Use of these names, trademarks and brands does not imply endorsement.

AGENDA

Introductions

Who is Team Cymru?

What is Network Hygiene

Why do we care ?

Bogon’s What are they

Prefix Filtering / RPKI

DDOS and Hygiene

Save / Make Money, Happy Customers

What can you do / Example Configs

Closing Comments

Questions ?

INTRODUCTIONS

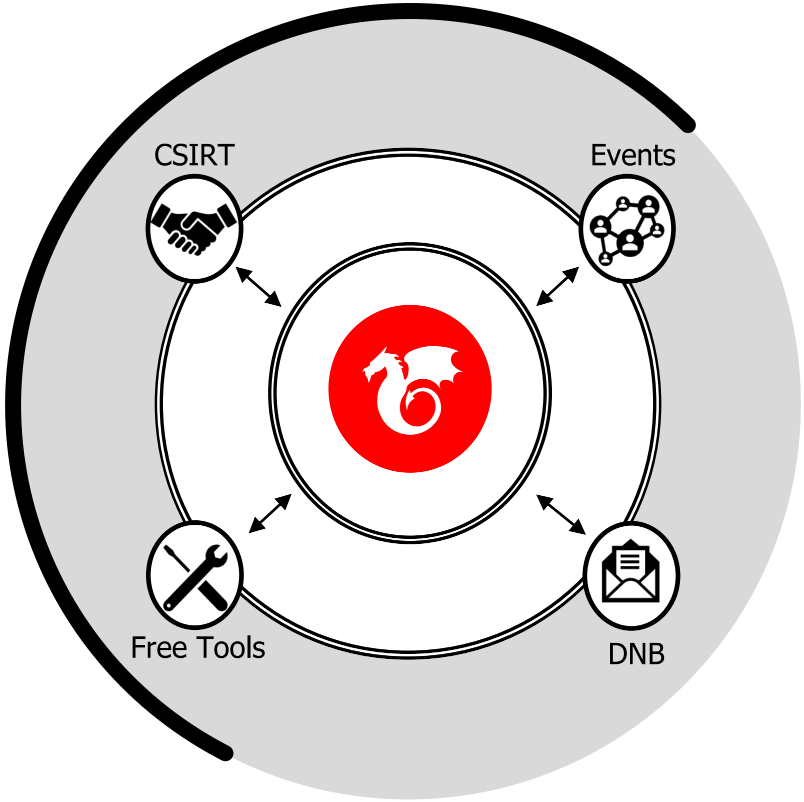
John Brown

- John Brown, CISSP, CFI, AGI, CP-AMEL
- Senior Security Evangelist at Team Cymru
- 35+ years as software and network engineer
- Principal Technical Engineer for ICANN’s L-Root DNS
- Have built Internet networks on 3 continents
- Recovering owner of a regional ISP business, ran it for 17 years
- Passionate about helping ISP’s improve their networks
- Past Mikrotik Authorized Instructor (MT-CNA, MT-CRE, MT-CINE)
- Past ISC2 CISSP Instructor
- Commercial Multi-Engine Pilot
- When not working, I enjoy building and flying airplanes…..

I can be reached at: jbrown@cymru.com

Who is Team Cymru ?

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

What is Hygiene

What is Hygiene

Hygiene is a series of practices performed to preserve health. According to the World Health Organization (WHO), "Hygiene refers to conditions and practices that help to maintain health and prevent the spread of diseases."

Basically the practice of keeping yourself clean and to help promote a health environment.

Each of us generally assumes that the person next to them is also interested in keeping healthy and not spreading diseases..

What is Network Hygiene

What is Network Hygiene ??

”Just as good personal hygiene is a prime contributor to personal (and community) health, good network hygiene is a major contributor to overall network health.” – Terry Slattery

Generally, if you keep YOUR network clean, then you AND your neighbors will have fewer problems. When a problem pops up it will also be easier to spot and resolve.

Back in 2006 Daniel Karrenberg (RIPE NCC) talked about a paper that Joao Damas wrote called “Network Hygiene Pays Off”….. Link in the references section of this talk

BCP 38 !! IP Spoofing!

- BCP 38. (Best Current Practice # 38)
- Published in May 2000 (23!!! YEARS AGO)
- A simple means to PREVENT Source Spoofed packets from entering the network.

- WHY AREN’T WE DOING IT ??
- By preventing SRC Spoofed packets from leaving your network you are helping your neighbors' network be safer.
- The technology can easily do it today!!

Other types of Network Hygiene

- Open NTP Servers – Can be used in Amplification attacks!

- Open Recursive DNS Resolvers – Can be used in amplification attacks!
    - Do you really need to provide recursive DNS services to the entire world ?????

- Improper IP Prefix filtering on BGP sessions (route hijacking, route redirection)

To name a few……

TEAM CYMRU

Why do we care ?

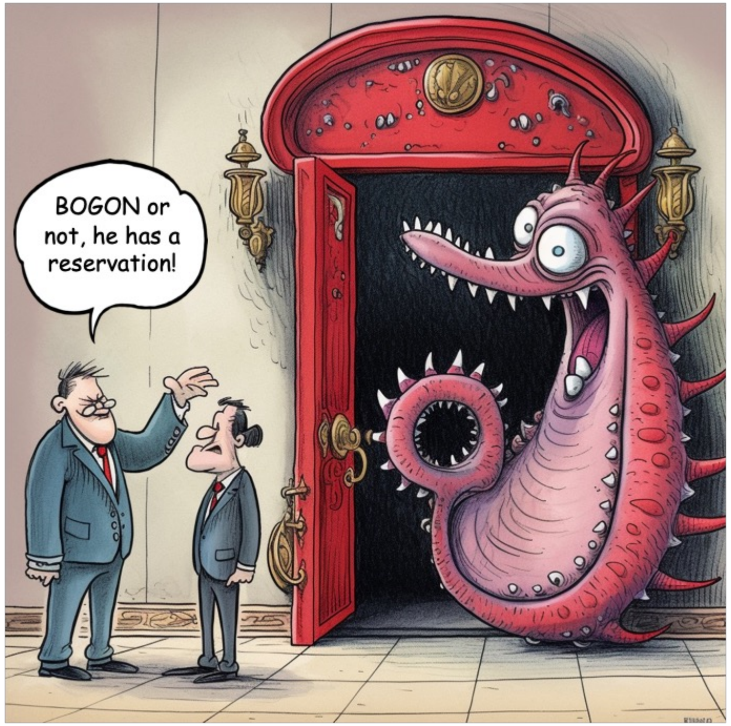
Why do we care ?

- Each of us network operators should care that our neighbor is also being responsible and practicing good network hygiene! Just as they wish that you do the same.
- Brushing your teeth everyday helps with the dentist visit (no or few cavities), keeping your network clean means fewer issues to solve when there is a really big problem.
- It is also about TRUST. Other network operators will trust your network more.

But its more than just other network operators….

- It is about CUSTOMERS (those people that pay you!)
- Knowing that your network runs with "Cleaner Pipes" is actually a REVENUE PLUS!!

Bogon’s – What are they ?



What are BOGON IP Prefixes

- **Traditional bogons** are **martians** (private and reserved addresses defined by RFCs) and prefixes that have not been allocated to a regional internet registry (RIR) by the Internet Assigned Numbers Authority (IANA)

- **Fullbogons** contain the traditional bogon prefixes, but also include the IP space allocated to the RIRs, but not yet assigned by them to Local Internet Registry's (LIRs), **for both IPv4 and IPv6**. These also contain prefixes that have been reclaimed or returned to a RIR.

- The Bogon Reference: https://www.team-cymru.com/bogon-networks

IP Martian Prefixes

IPv4 Martians

0.0.0.0/8	# RFC 1918 private space
10.0.0.0/8	# RFC 1122 'this' network
100.64.0.0/10	# RFC 6598 CG NAT space
127.0.0.0/8	# RFC 1122 localhost
169.254.0.0/16	# RFC 3927 link local
172.16.0.0/12	# RFC 1918 private space
192.0.2.0/24	# RFC 5737 TEST-NET-1
192.88.99.0/24	# RFC 7526 6to4 anycast relay
192.168.0.0/16	# RFC 1918 private space
198.18.0.0/15	# RFC 2544 benchmarking
198.51.100.0/24	# RFC 5737 TEST-NET-2
203.0.113.0/24	# RFC 5737 TEST-NET-3
224.0.0.0/4	# multicast
240.0.0.0/4	# reserved

IPv6 Martians

::/8	# RFC 4291 IPv4-compatible, loopback
0100::/64	# RFC 6666 Discard-Only
2001:2::/48	# RFC 5180 BMWG
2001:10::/28	# RFC 4843 ORCHID
2001:db8::/32	# RFC 3849 documentation
2002::/16	# RFC 7526 6to4 anycast relay
ffe::/16	# RFC 3701 old 6bone
fc00::/7	# RFC 4193 unique local unicast
fe80::/10	# RFC 4291 link local unicast
fec0::/10	# RFC 3879 old site local unicast
ff00::/8	# RFC 4291 multicast

What are Bogon ASN’s (Autonomous System Numbers)

- Similarly, to prefixes, an ASN should be termed as Bogon **if any of the following conditions is true.**
  - It is reserved for special use by an RFC
  - It is not part of the block assigned to a RIR by IANA
  - It is not assigned to a LIR by any RIR

- https://www.manrs.org/2021/01/routing-security-terms-bogons-vogons-and-martians/

Reserved ASN’s

0	# RFC 7607
23456	# RFC 6793 AS_TRANS
64496 – 64511	# RFC 5398 and documentation/example ASNs
64512 – 65534	# RFC 6996 Private ASNs
65535	# RFC 7300 Last 16 bit ASN
65536 – 65551	# RFC 5398 and documentation/example ASNs
65552 – 131071	# IANA reserved ASNs
151866 – 196607	# Unallocated
213404 – 262143	# Unallocated
273821 – 327679	# Unallocated
329728 – 393215	# Unallocated
401309 – 4199999999	# Unallocated
4200000000 – 4294967294	# RFC 6996 Private ASNs
4294967295	# RFC 7300 Last 32 bit ASN

Why do we care about Bogon’s in the global BGP ?

- Generally, they are the results of a misconfiguration on a network router.
- However, these prefixes can be **and are** used for malicious activity.
- Bogon’s can be used for DDOS.
- Bad Actors know that these prefixes aren’t “traceable” since they are not registered to a proper ORG.
- But because they are in the global routing tables, they can be used (short term) for TCP based attacks. Those attacks may be limited in “scope” or network reach…
- Bogon AS’s can be used for Route Hijacks, Route Leaks.

Looking into BGP data

- Team Cymru partnered with CodeBGP to look into their BGP view.
- Using Code BGP's global BGP Monitoring tools we see:
  - Hundreds to Thousands of announcements of BOGON IP's and ASN's
  - Actual BOGON IP's (reserved, unallocated by RIR, special use addresses)
  - AS Numbers that are being used to provide TRANSIT to other networks, and those AS Numbers are not assigned in any RIR database. (These are not reserved ASN's)
  - Reserved AS Numbers that are providing TRANSIT, they are in the middle of an AS PATH
  - Data at RIR's that is not up to date, or is missing..

- Criminals love this because it makes it harder to track and catch them!
- Our research and investigation is ongoing. More to come……….

Prefix Filtering / RPKI

What steps can we take ?

- ISP’s should
  - Validate their external facing route filters.
  - Make sure your IRR database entries are UP TO DATE AND CORRECT!
  - Make sure you are ONLY announcing prefixes that are valid.
  - You MUST filter what your BGP downstream peers send you!!! (Yes, it can be a pain)
  - Set up a TEST router to see what you are actually sending. You could use a Mikrotik or Exa-BGP or similar…
  - Make use of Team Cymru’s BOGON BGP feed (real time updated) to drop traffic
    - Make sure you understand how this works and don’t drop internal traffic.
- RIR’s should make sure that their ASN and IP records are updated. If an ASN isn’t assigned it should be marked as UNASSIGNED and not just blank…..

Make use of RPKI

- Make sure YOUR prefixes are properly signed with the appropriate RIR(s).
    - This will help tell your neighbors that these are really YOUR prefixes!!
    - APNIC, RIPE, LACNIC, ARIN, AfriNIC all have well documented and easy processes here!!! They are happy to help.
- Start using RPKI to validate routes YOU RECEIVE from others.
    - Maybe start with peering / IX's first, then move towards transit providers

DDOS and Network Hygiene

DDOS and Network Hygiene

- By preventing Source Spoofed packets from leaving your network….
  - You help yourself AND the person sitting to your left and/or right!!!!

- If we didn't have Source Spoofed Packets a HUGE amount of DDOS would evaporate from the planet.

- Stop Source Spoofed IP packets and become an Internet Hero!!
- Actively check and remove public facing services that can be abused for DDOS
  - (Recusive DNS, NTP, CharGen, etc)

Save / Make Money, Happy Customers

Money Money Money

- The cost of running a network is far more than routers, switches, peering, transit, power, hvac, and people
- You have a cost to get customers
- You have a cost when a customer leaves your service
- You have a cost when in the middle of the night your network engineering folks are woken up to solve a problem.

- Proper / Good Network Hygiene will reduce your operational costs.

Money Money Money

- A business improves is profit by making changes to, two places on the balance sheet!
- Top of the balance sheet (INCOME, more sales, etc)
- Bottom of the balance sheet (EXPENSES, less expenses)
- Change either of these in the right direction and you get more profit!!
- Change BOTH of them, and well, life is good!!
- You can actually MARKET that you have a clean network.
- When you read a review about a restaurant, “Good Food, Clean Environment, friendly staff…”
  - They are selling HYGIENE!!!

What can you do / Example Configs

What can you do ??

To Quote Joao Luis Silva Damas

Good Practice is Not Hard

It is not hard to prevent such a scenario. You simply have to do BCP38 towards your customers and drop all packets with internal source addresses coming in from external peerings.

Once you have done that you *know* exactly who has sent a packet with an internal source address and you also know that any packet with an external source address must have come in via one of the external peerings.

Some multi-homing customers or customers using certain types of mobile IP may require special configuration efforts. However these are neither impossible nor very costly if implemented well.

Some recommendations on things to do

- Implement BCP 38
- Filter announcements TO/FROM a peer or IX and prevent BOGON's
- IX's can use the TC BOGON's service (no cost) to make sure such traffic is dropped on MLPA / Route-Server configurations.
- Make use of FREE Open Community tools like Team Cymru's:
  - BOGON's,
  - UTRS (DDOS Mitigation)
  - Nimbus (Near real-time Threat Intelligence Information)
- Work in your community to help other ISP's improve their network hygiene.

Mikrotik ROS v7.x Sample Bogon Config

```
/routing bgp template
          set default address-families=ip as=<YOUR_ASN> disabled=yes multihop=yes router-id=<YOUR_IP> routing-table=main
          add address-families=ip as=<YOUR_ASN> disabled=no input.filter=TC-BOGONS-IN
                    multihop=yes name=TC-BOGON-TEMPLATE nexthop-choice=force-self router-id=<YOUR_IP> routing-table=main
```

Mikrotik ROS v7.x Sample Bogon Config

```
/routing bgp connection

          add address-families=ip as=<YOUR_ASN> disabled=no input.filter=TC-BOGONS-IN
                    local.address=<YOUR_IP> .role=ebgp multihop=yes name=bogonrs02
                    nexthop-choice=force-self remote.address=<BOGON_SERVER_IP> .as=65332
                    router-id=<YOUR_IP> routing-table=main templates=TC-BOGON-TEMPLATE
/routing filter rule
          add chain=TC-BOGONS-IN disabled=no rule="if (dst==192.168.0.0/16) {reject;}"
          add chain=TC-BOGONS-IN disabled=no rule="if (bgp-communities includes 65332:888)
          {set distance 1; set gw 192.0.3.1; append bgp-communities no-export,no-advertise;
          set blackhole yes;  accept;}"
```

Closing Comments

Closing Comments

- As Network Engineers and Operators we are responsible for our network hygiene
- Take the time to validate routes received from neighbors, including the origin ASN
- Take the time to validate what you are sending to your BGP peers / neighbors
- This is not a one time process. It must constantly be reviewed and audited!

Please don’t run smelly networks ☺

- If you need help with possible configuration examples, reach out. outreach@cymru.com

Questions ??

References

- https://www.ripe.net/ripe/mail/archives/spoofing-tf/2006/msg00022.html
- https://netcraftsmen.com/the-importance-of-good-network-hygiene/
- https://www.flickr.com/photos/dapuglet/8426525097
- https://creativecommons.org/licenses/by-sa/2.0/
- https://www.ietf.org/rfc/bcp/bcp38.html

How we can help cybercrime by understanding the social/economic drivers of why people get into cybercrime.

- ”Mapping the Global Geography of Cybercrime”

- Research by the University of Oxford

- Dr. Miranda Bruce
- Miranda.bruce@sociology.ox.ac.uk

THANK YOU