Data, Data Everywhere, and now to stop and think

Leslie Daigle

CTO, Global Cyber Alliance

RIPE MAT WG, May 2022

GLOBAL CYBER ALLIANCE™

What I’d like to talk about today…

What can we do about the vast amount of unwanted (attack) traffic on the Internet today, given that we can pinpoint many of the sources

- Without breaking the Internet
  - I.e., not a great big IP block list

Overview

- Why do we (all) care
- Some perspectives on just how much attack traffic is out there
  - This is a bit of a logical follow on to George Michaelson’s presentation at RIPE 83
- What does “Bad” look like?
- Discussion
  - What is “acceptable” levels
  - Thoughts on how to get there

Why do we (all) care

- Who remembers October 21, 2016?
  - MIRAI botnet distributed denial of service attack on Dyn services
  - https://en.wikipedia.org/wiki/DDoS_attack_on_Dyn
- Aka – why so many laws against default passwords…
- Of course, it’s not all about conscription of devices into the world’s largest botnet
- The same actors are hitting everything (at least in IPv4 space)
  - Some are getting toe-holds on edge devices and escalating within networks

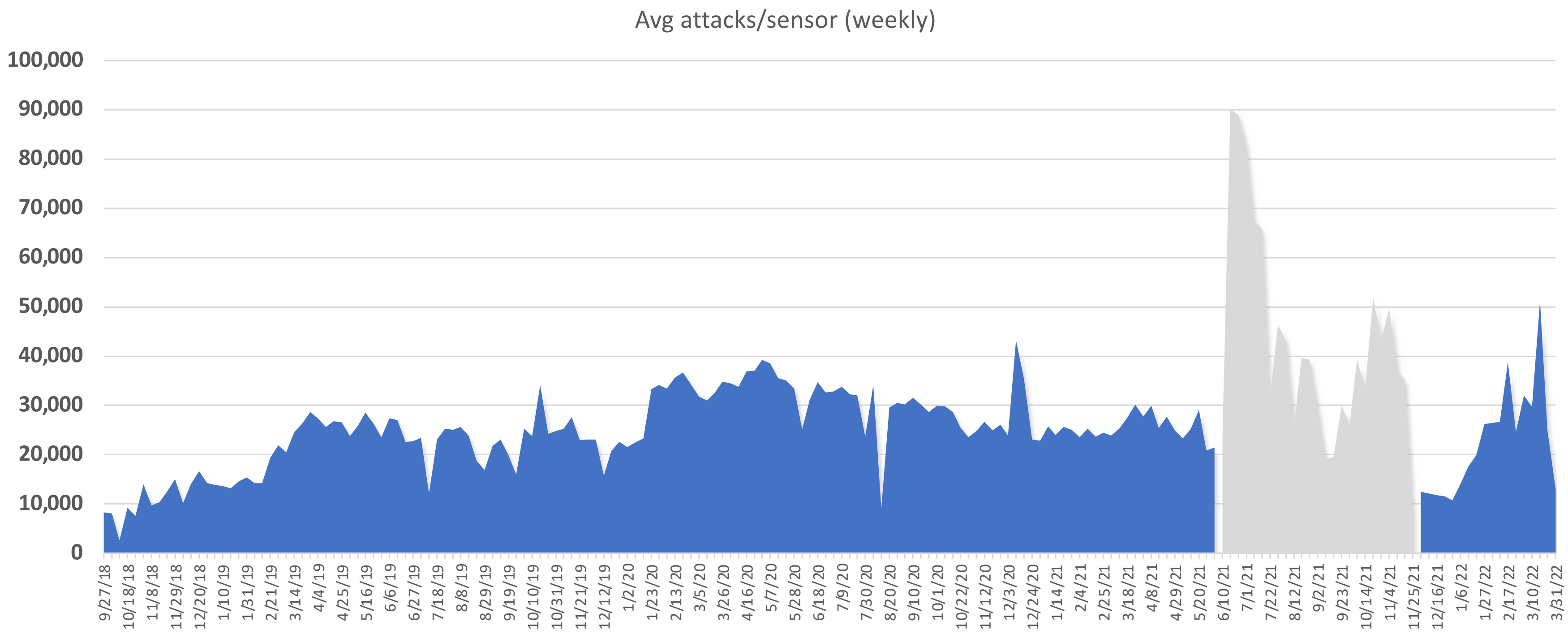
Why do we (GCA) care

- Global Cyber Alliance
  - Not for profit
  - Dedicated to reducing cyber risk
- GCA AIDE project includes
  - global honeyfarm (hundreds of sensors)
  - 4 years of data
  - Other cool tech, not part of this discussion :^)

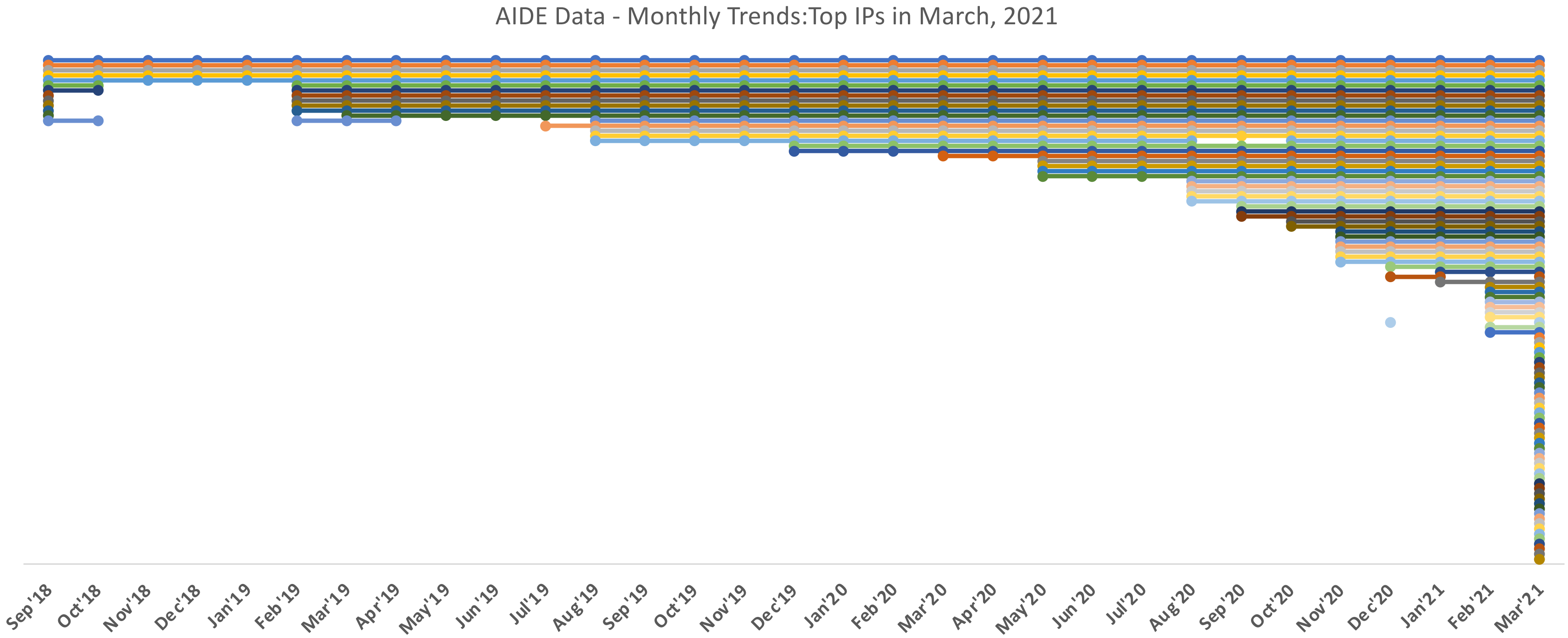
How big is this?

With Charts from Rufo De Francisco

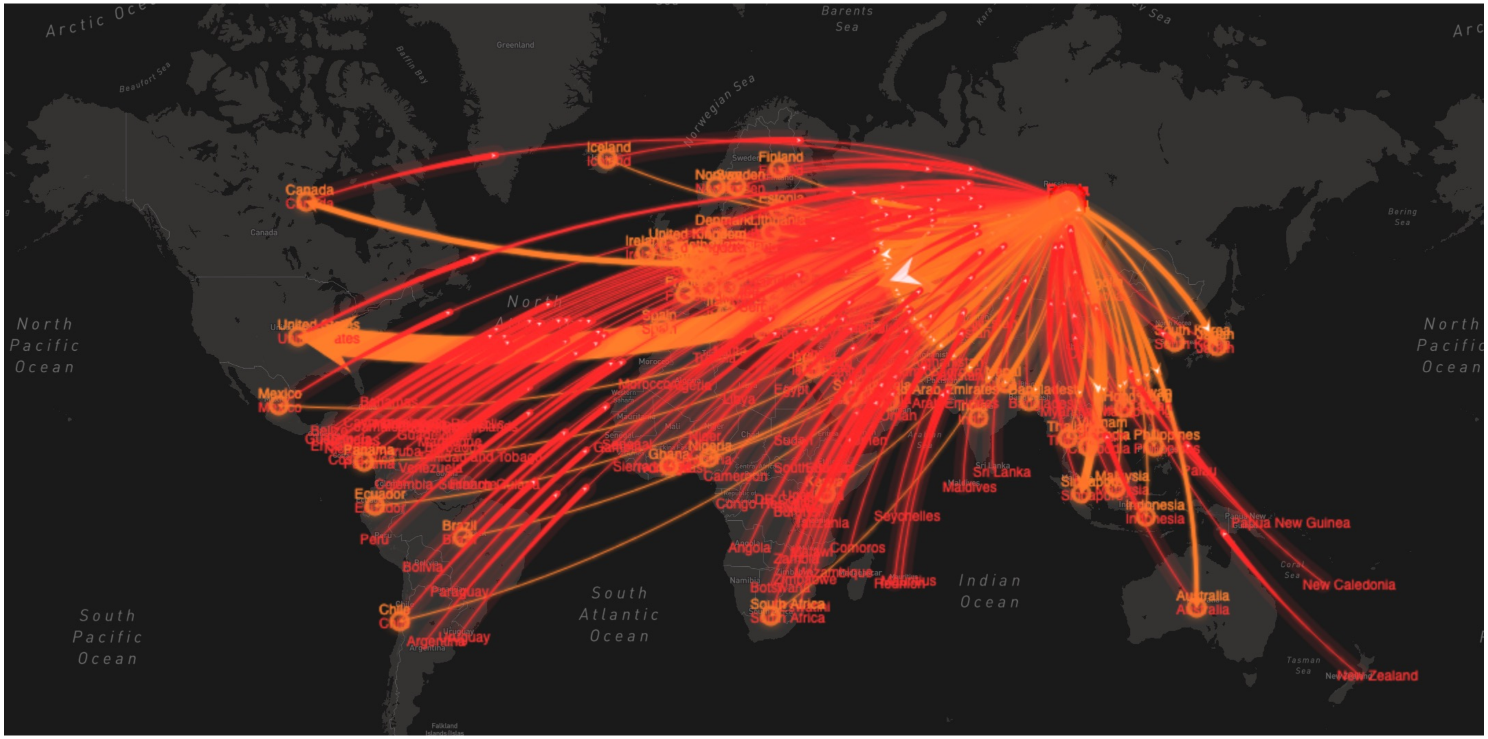
Attacks per sensor



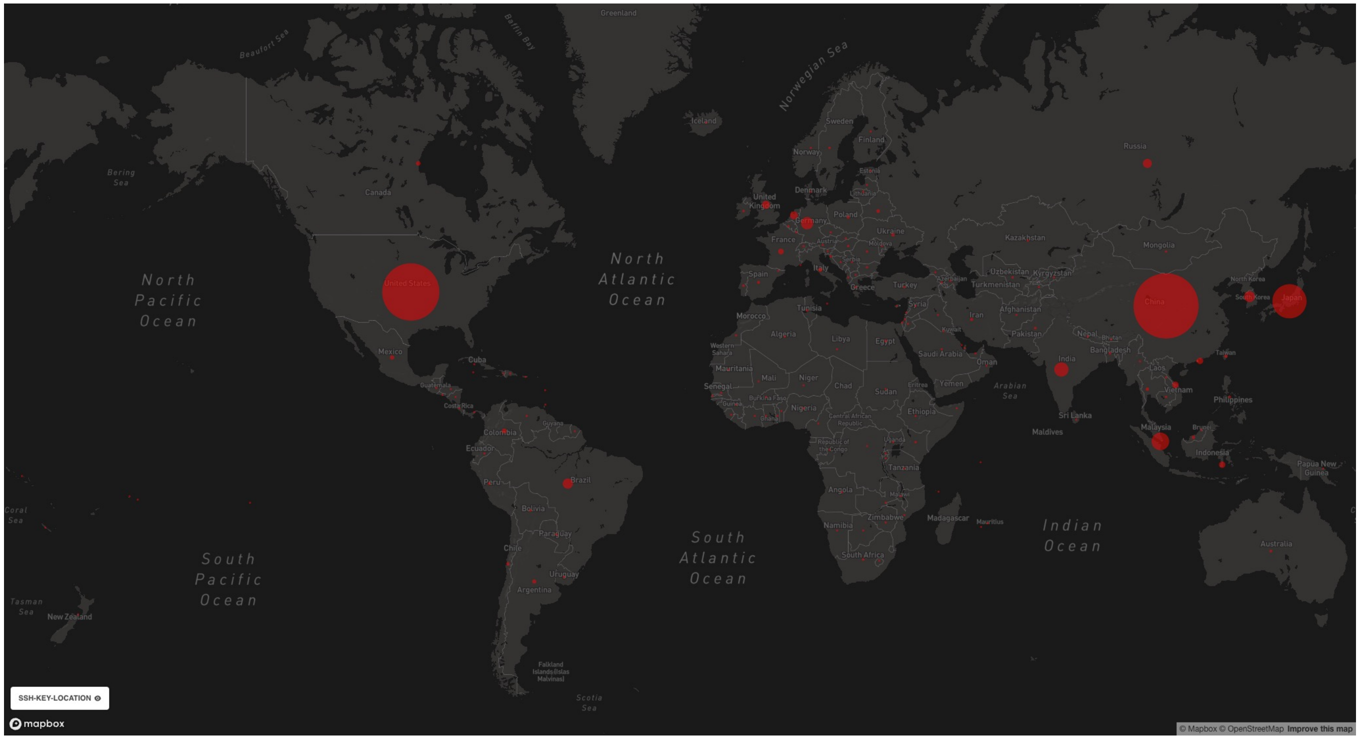
Some players just don’t quit



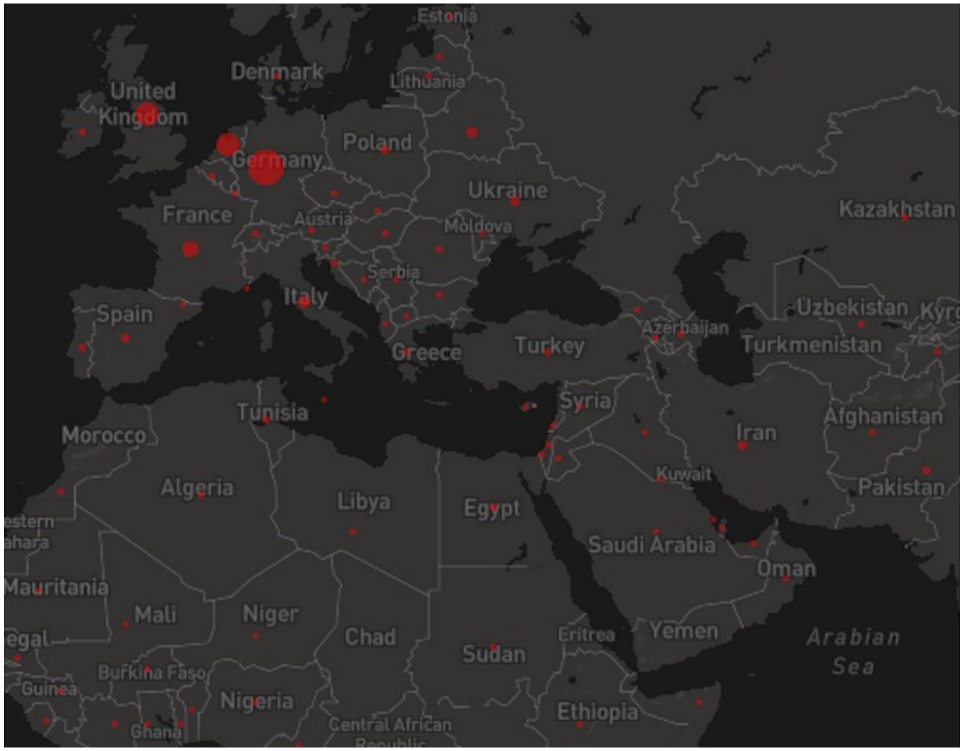
March 2022 – Attacks to/from Russia



One attacker’s global footprint



Closeup


Estonia
Denmark
Lithuania
United Kingdom
Poland
Germany
Ukraine
Kazakhstan
France
Austria
Moldova
Serbia
Italy
Spain
Azerbaijan
Uzbekistan
Kyrg
Turkey
Turkmenistan
Greece
Syria
Afghanistan
Tunisia
Morocco
Iran
Kuwait
Pakistan
Algeria
Libya
Egypt
estern
ahara
Saudi Arabia
Oman
Mauritania
Mali
Niger
Chad
Sudan
Eritrea
Yemen
Arabian Sea
egal
Burkina Faso
Guinea
Nigeria
Ghana
Central African Republic
Ethiopia

Some observations

- That’s a lot of attack traffic hitting each sensor (any host on the network)
- Some players are persistent
- It’s from everywhere, to everywhere

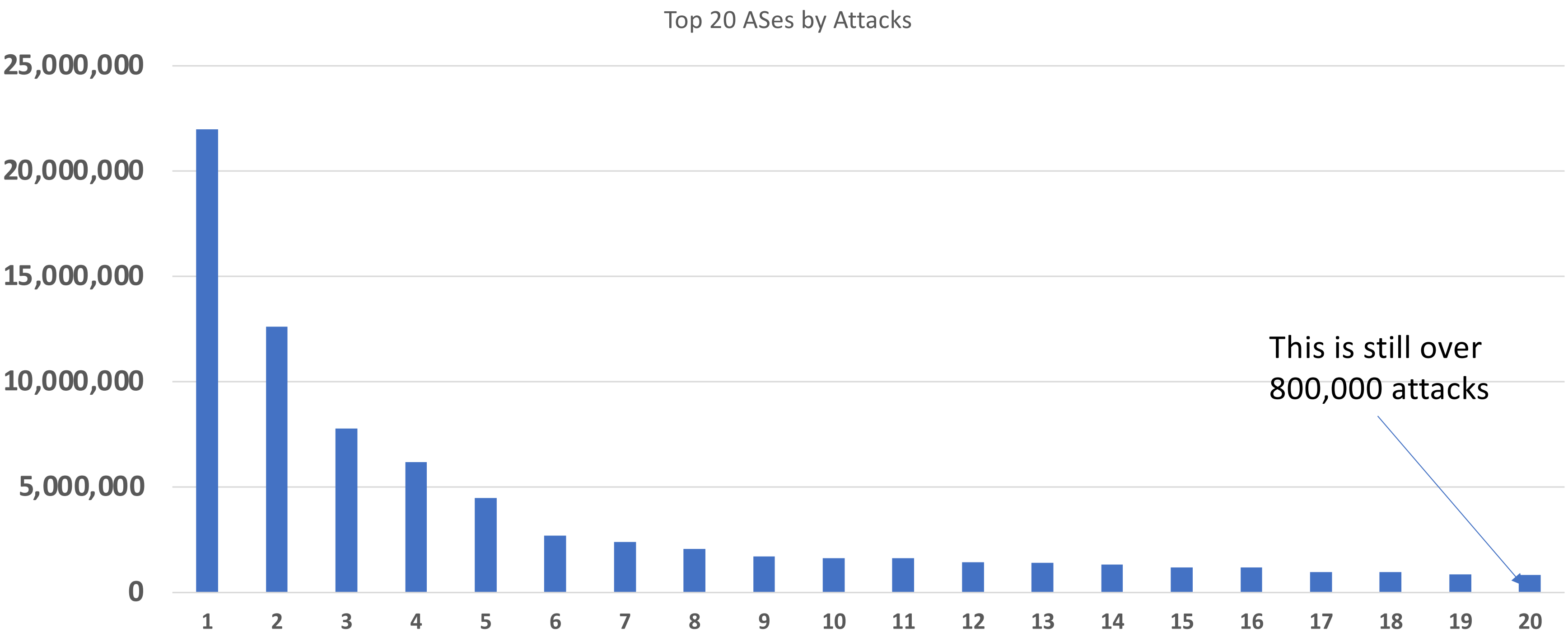
What does “Bad” look like?

November 29, 2021 to May 8, 2022 – 160 days

Some stats (from that timeframe)

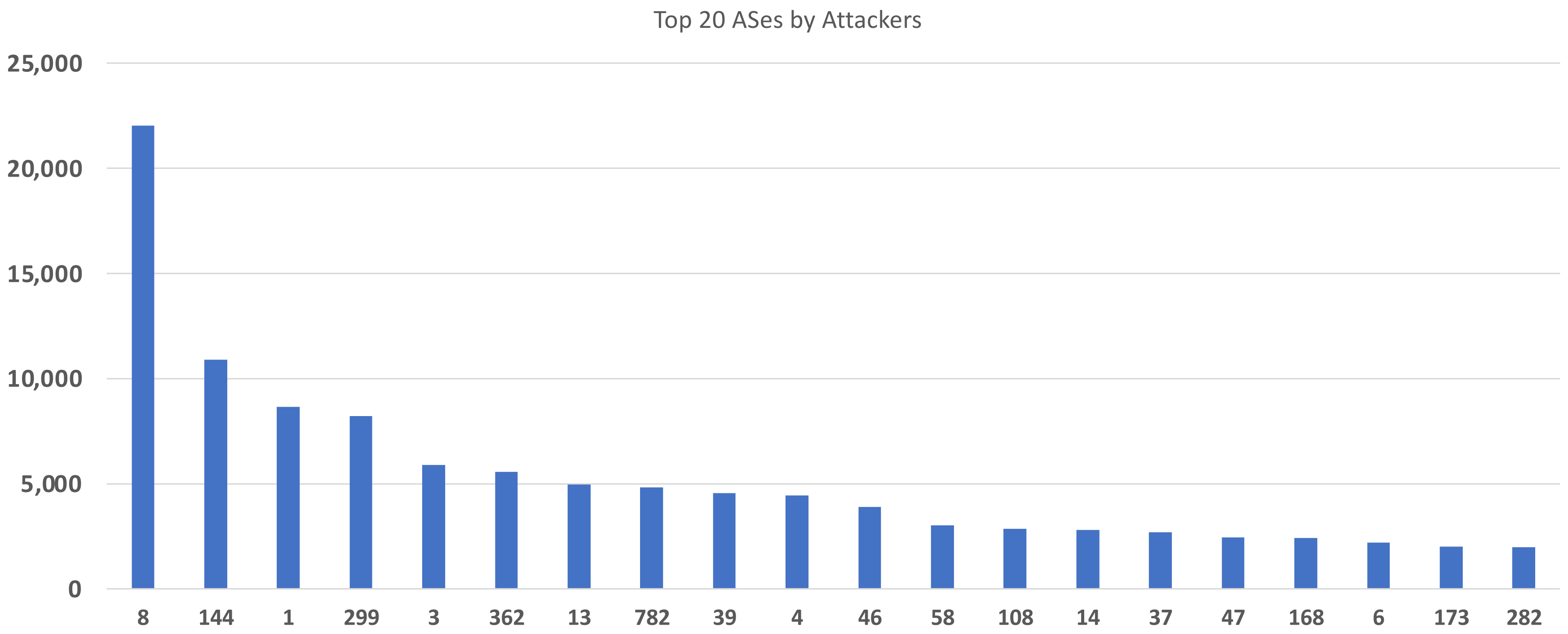
- Our ~200 sensors saw attacks from
  - 10,823 ASes
    - 2,183 of them fielded more than 1,000 attacks on our sensors
    - 40 of them launched attacks from more than 1,000 distinct IP addresses
  - 274,494 distinct IP addresses

Numbers of attacks



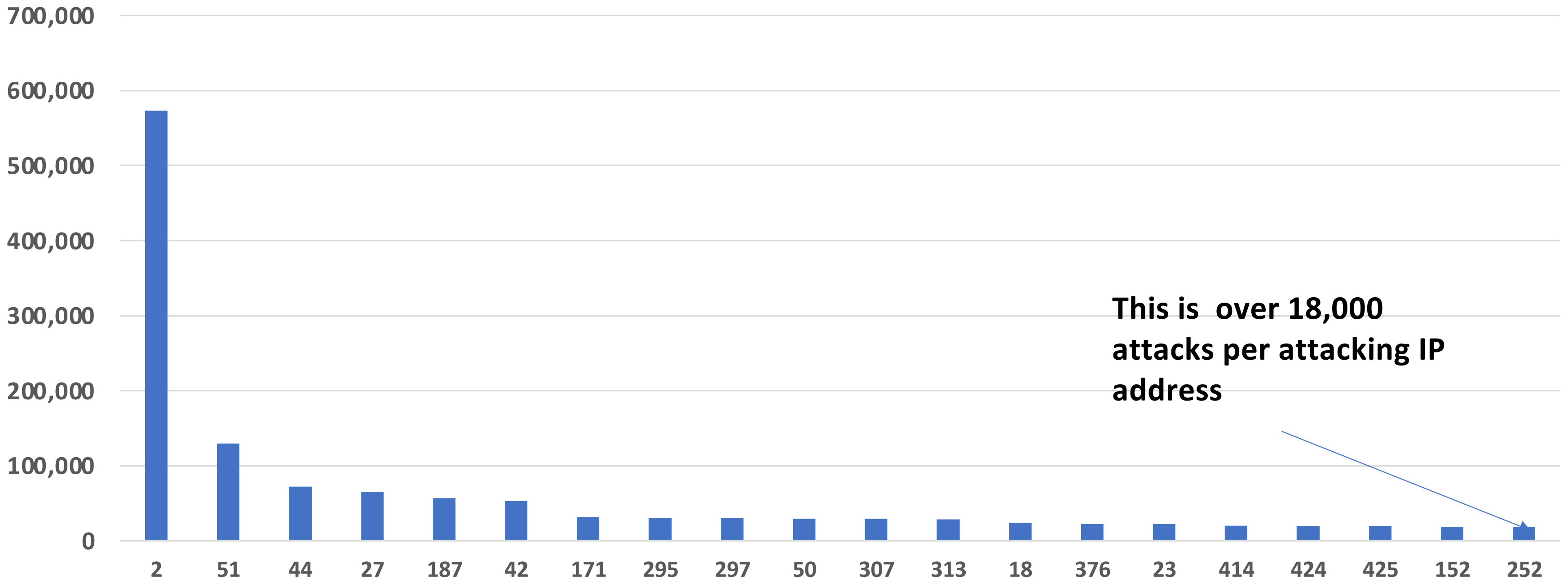
This is still over 800,000 attacks

Number of Attackers



Activity of Attackers

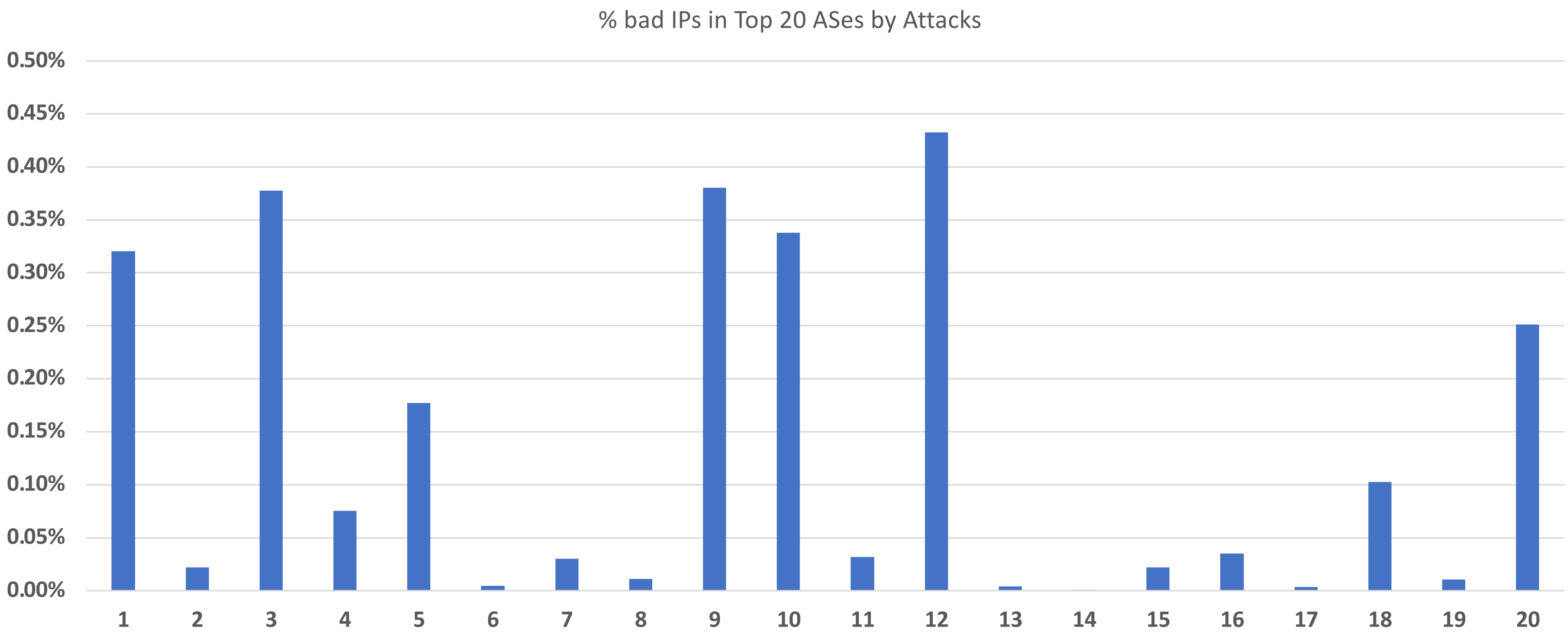
Top 20 ASes by Attacks per Attacker



This is over 18,000 attacks per attacking IP address

Percentage of bad actors in a network

(Based on addresses per AS data from https://bgp.he.net)



To note

- The network IDs are not the same in every graph
  - The network with the most (raw) attack traffic didn’t have the greatest number of attacking IP addresses
- Level of IP address bad behaviour is small (less than 1% of network) and highly variable

So…

What I want you to conclude…

- This much rampant attack traffic isn’t right
- Reducing the amount is better than (strictly) trying to prevent impact
  - Not interested in building the world’s biggest IP block list
    - But somebody will
  - Only a limited amount of early detection unless we can pick out clues from the malware (hashes)
- It would be better to stop at source – not all of this activity is condoned by the network operator

Discussion

- What’s worst
  - Raw number of attacks coming out of an AS?
  - Number of attacks coming from a single IP address?
  - Proportion of IP addresses acting badly?
- What’s detectable (in network operations)
- What’s “acceptable”?
  - Levels of the metrics above
  - Length of attack streak
- What can/should be done for “unacceptable”?

- And see me if you want to know what we get from your AS :->

Thanks!

Further thoughts? ldaigle @ globalcyberalliance.org