Reeling in Unwanted Traffic

Phil Roberts, Global Cyber Alliance

NANOG 88, June 2023

GLOBAL
CYBER
ALLIANCE™

Who we (GCA) care

- Global Cyber Alliance
  - Not for profit
  - Offices in the US, UK, Europe, Singapore
  - GCA’s mission: A Trustworthy Internet
  - At GCA we build programs, partnerships, and tools to make the connected world safer and more secure for all

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(of APNIC) 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

GCA’s Automated IoT Defense Ecosytem (AIDE)

- Platform that collects and analyzes attacks on IoT devices
- Will be part of mechanisms of distributed defense within the IoT community
  - Manufacturers, network operators, researchers, regulators, smart cities, consumers
- Three existing components:
  - The honeyfarm, an at scale, worldwide distributed network of honeypots
  - ProxyPot, proprietary technology to capture traffic to/from both physical and emulated devices
  - A data visualization and analysis platform based on OpenSearch

AIDE Honeyfarm(1)

- Hundreds of identical sensors based on an open-source honeypot
- Emulates Linux systems commonly found in IoT devices
- Captures traffic over Telnet and SSH
  - Peer (attacker) and host (sensor) IP and port, credentials, commands, malware files and URLs
  - From IPs, we get geolocation and ASN info using MaxMind
  - From malware hashes, we get malware information using VirusTotal

AIDE Honeyfarm(2)

- Operating since September 2018
- Two versions with an overlapping transition
  - Honeyfarm1: September 2018 through June 2022: 1,200 sensors mainly in Europe and the US
  - Honeyfarm2: December 2021 to now: 200 sensors with better geographical balance

ProxyPot Honeyfarm

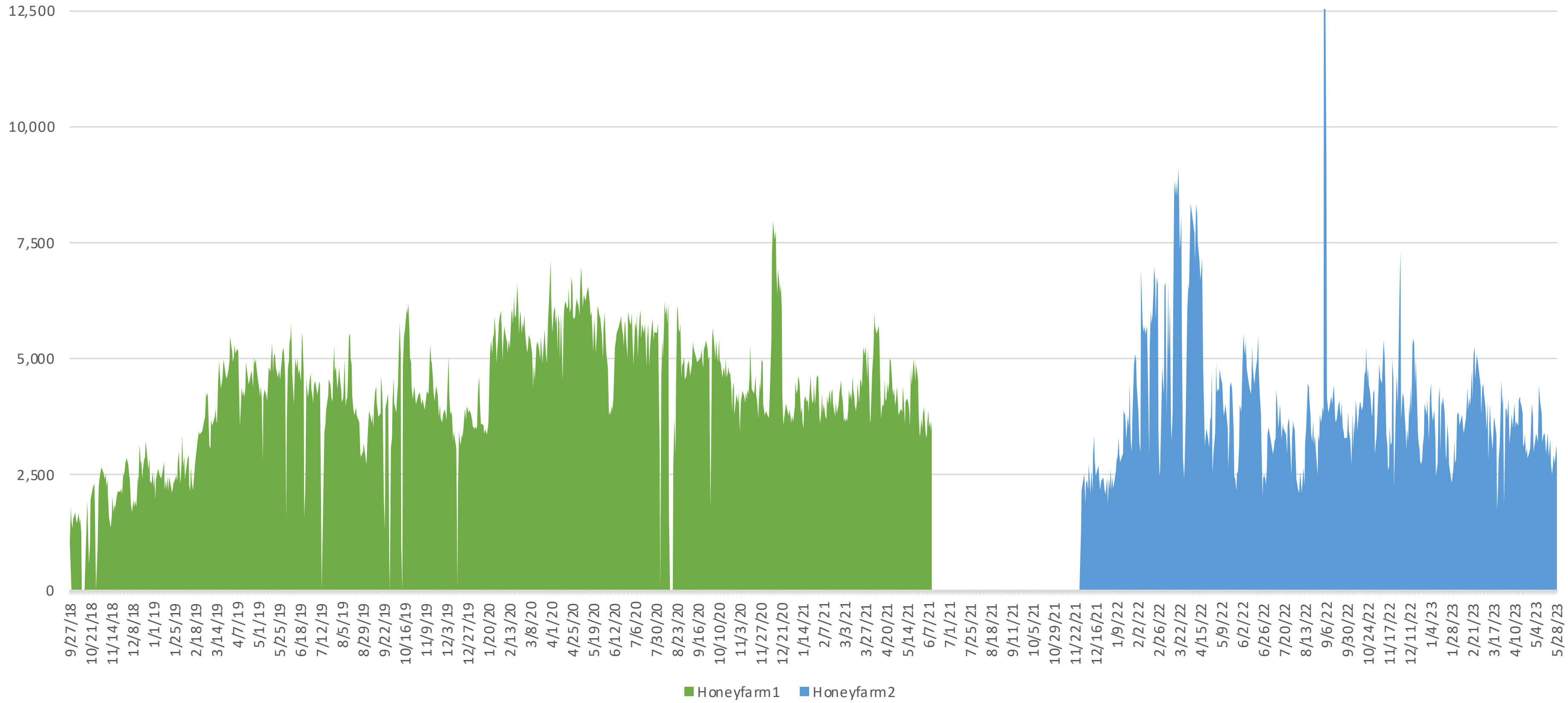
- ProxyPot is effectively a proxy server that sits between devices (physical or emulated) and the Internet
- It captures traffic to/from devices (PCAP)
- Typically used to run short-term (as in a few months) data collection exercises. E.g.:
  - Assess vulnerability of particular physical devices
  - Perform A/B testing (e.g., some devices configured with some controls enabled, the same devices configured with those controls disabled)
- Currently running a physical honeyfarm of 100 real IoT devices

How big of a problem is this?

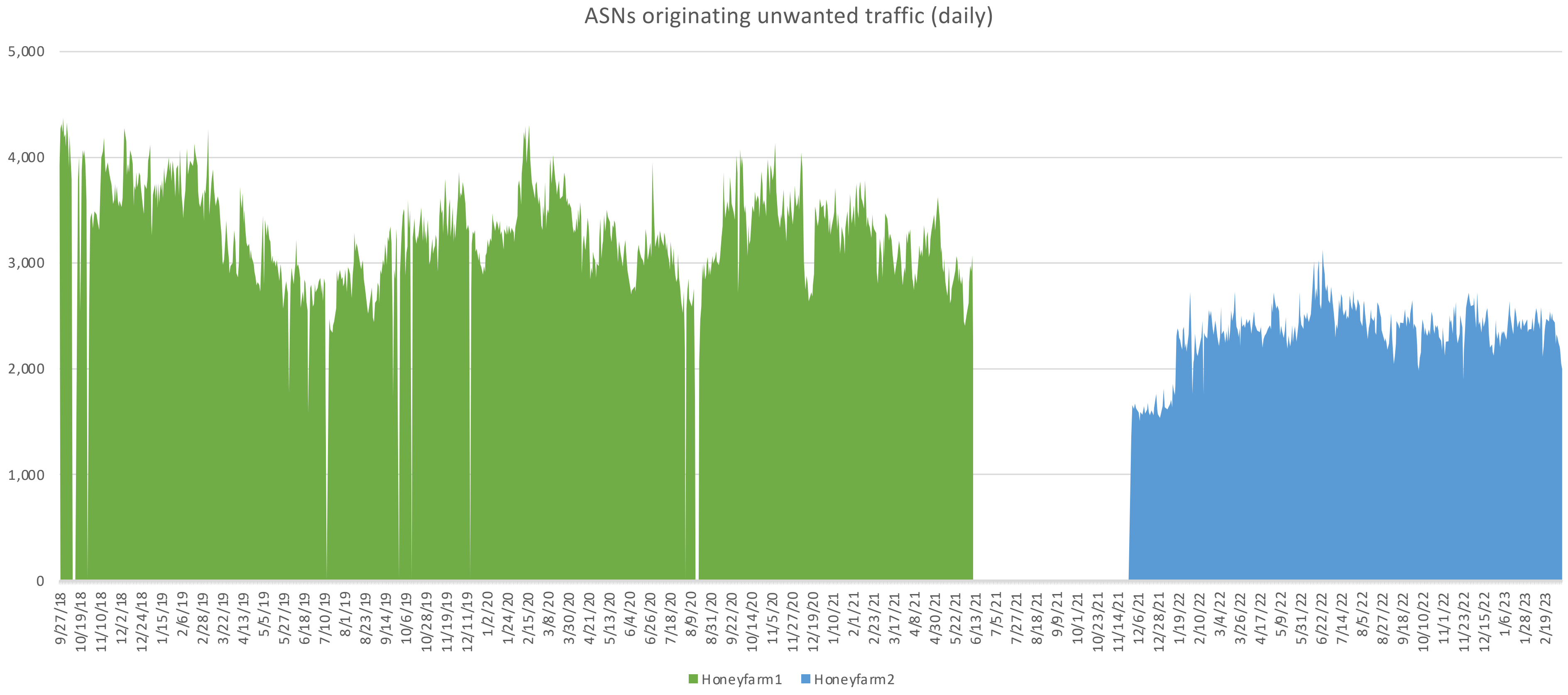
With charts and data from Rufo De Francisco

Attacks per sensor

Avg attacks/sensor (daily)

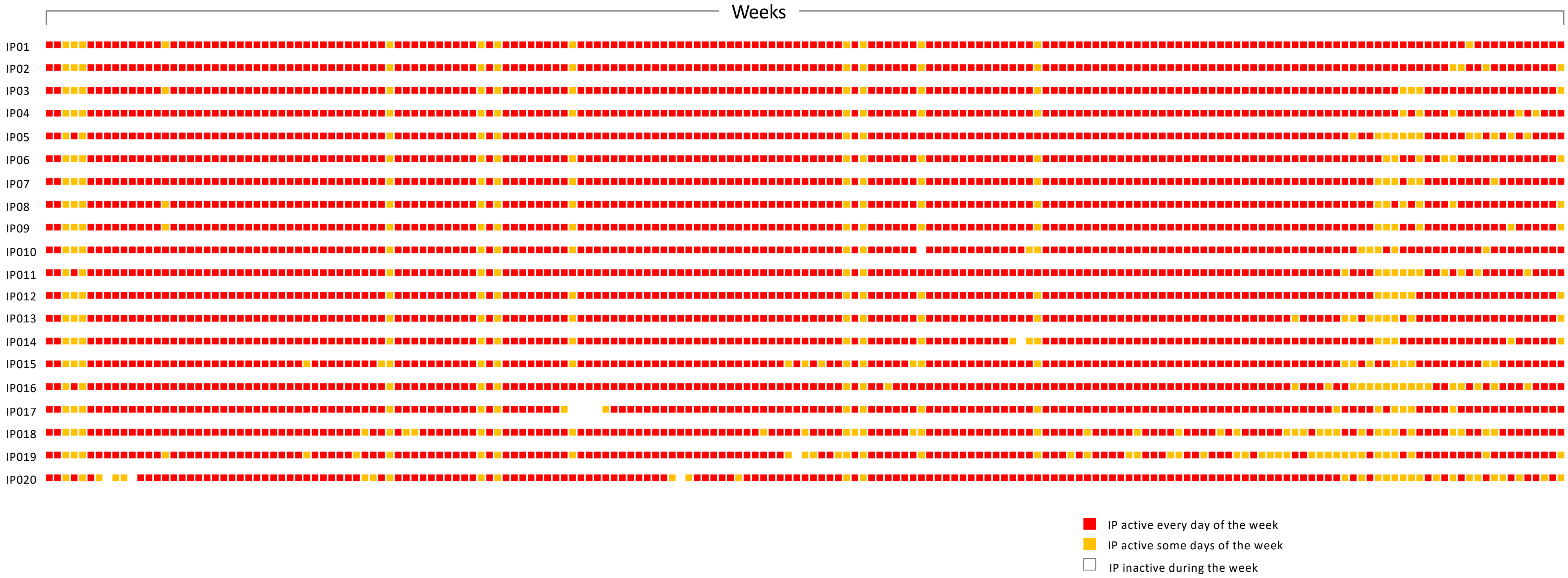


Networks involved

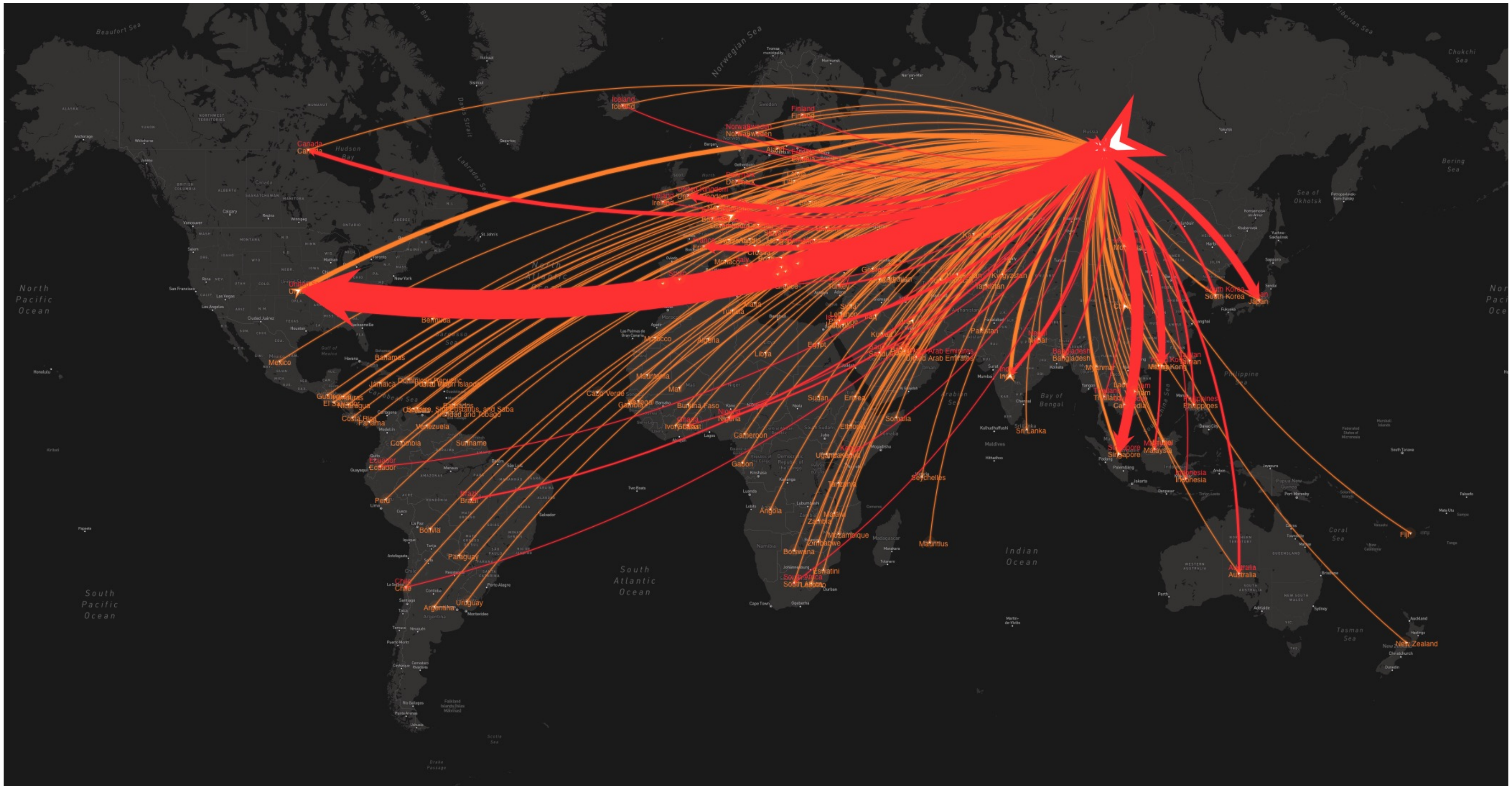


ASNs originating unwanted traffic (daily)

Some players just don’t quit



May 2023 – Attacks to/from Russia



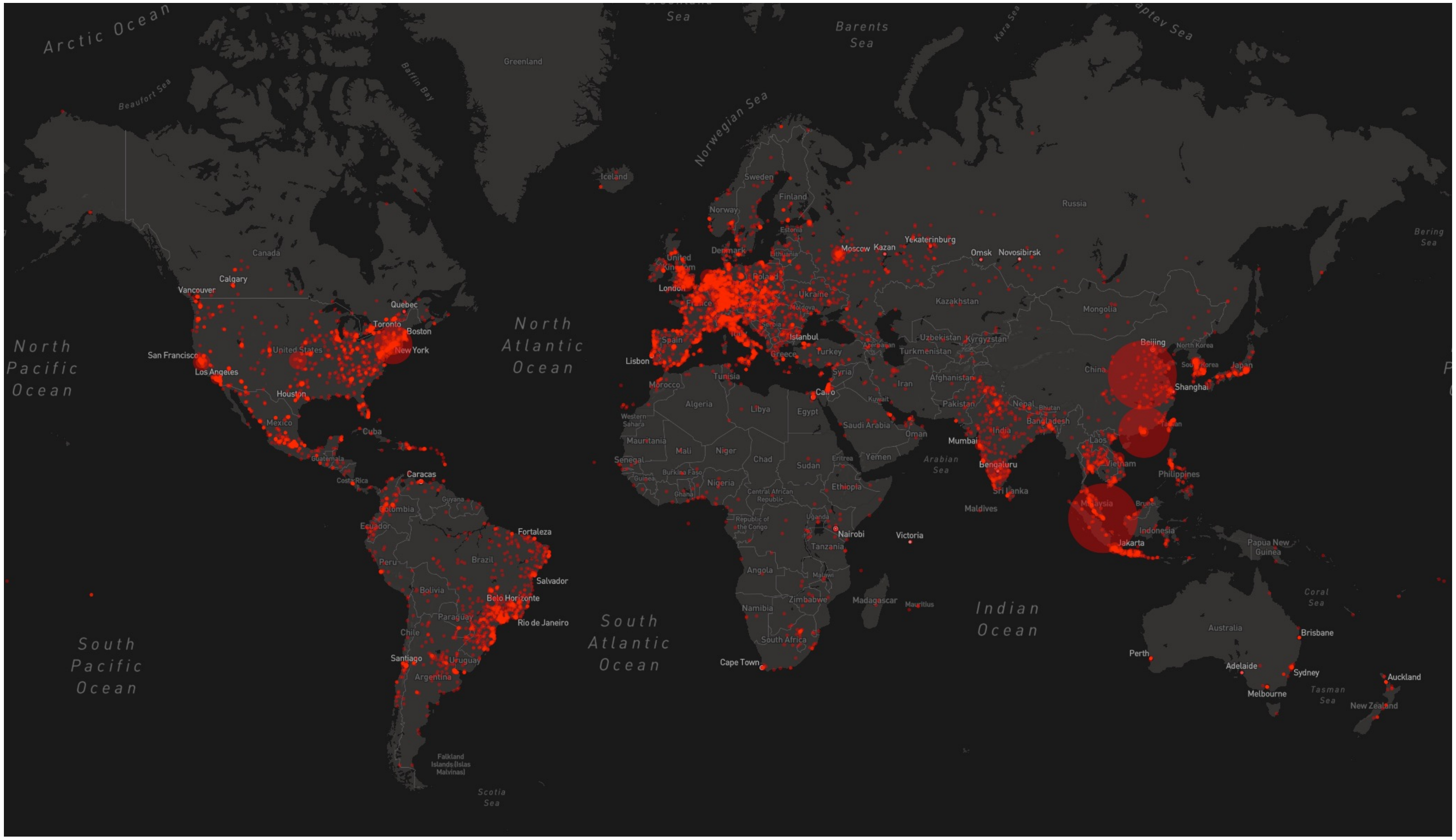
Max: 147,954 attacks from RU to US

206 sensors in 54 countries

Sensors in US: 53

Sensors in RU: 3

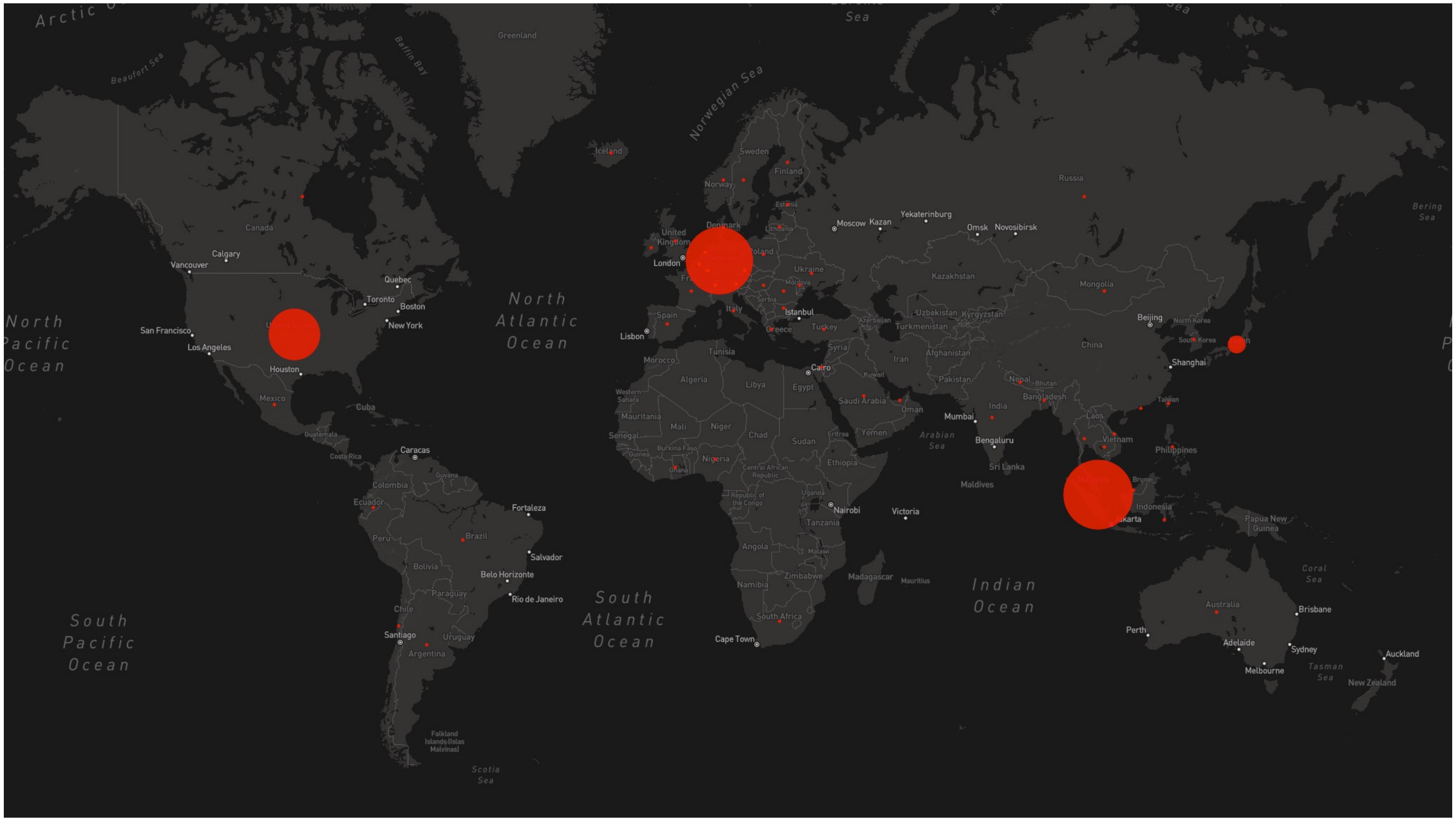
One attacker’s global footprint



28M identical attacks (i.e., same malware payload*) from 129K IPs in 8K locations across the world

* Trojan shell script + miner

Another attacker’s global target surface



IP geolocated in NL
Launched 5.4M attacks targeting sensors in all 57 countries
Max: 1.9M attacks on SG

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

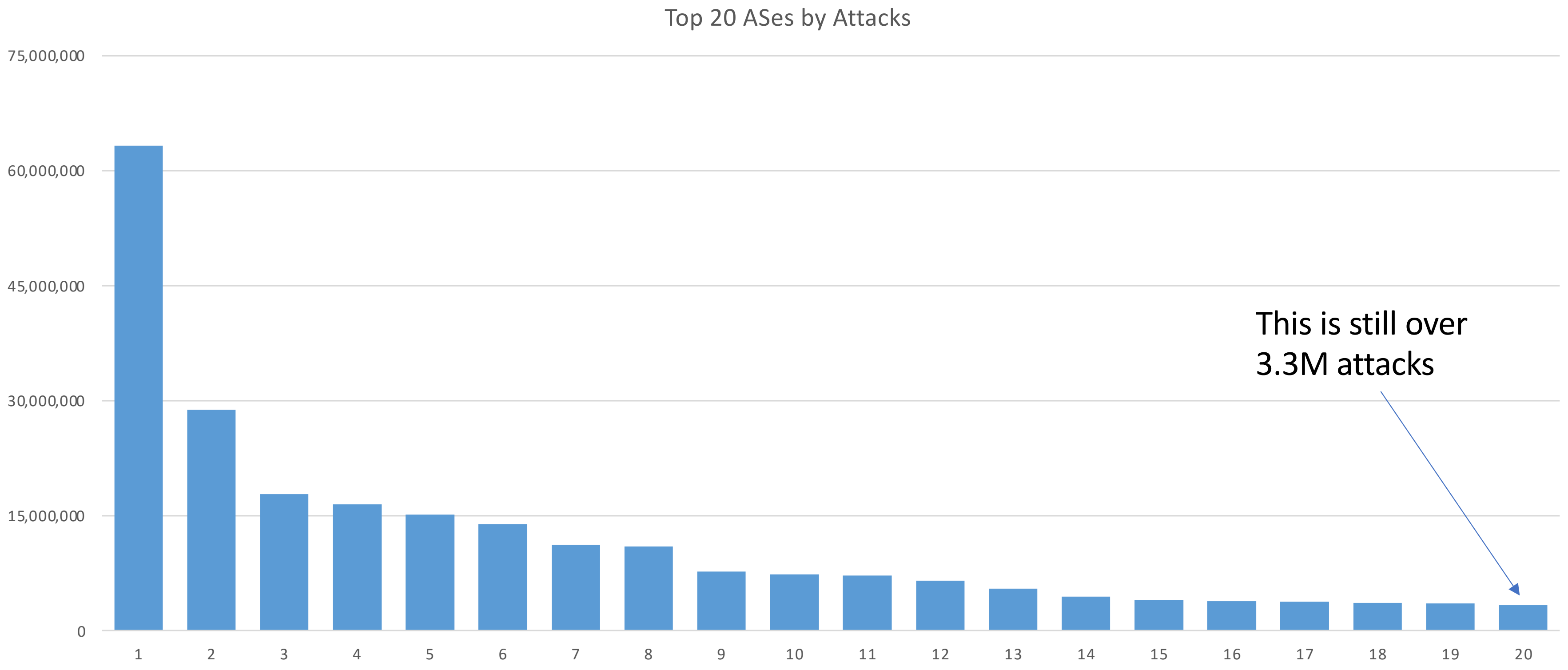
What does “Bad” look like?

November 29, 2021 to May 30, 2023 – 547 days

Some stats (from that timeframe)

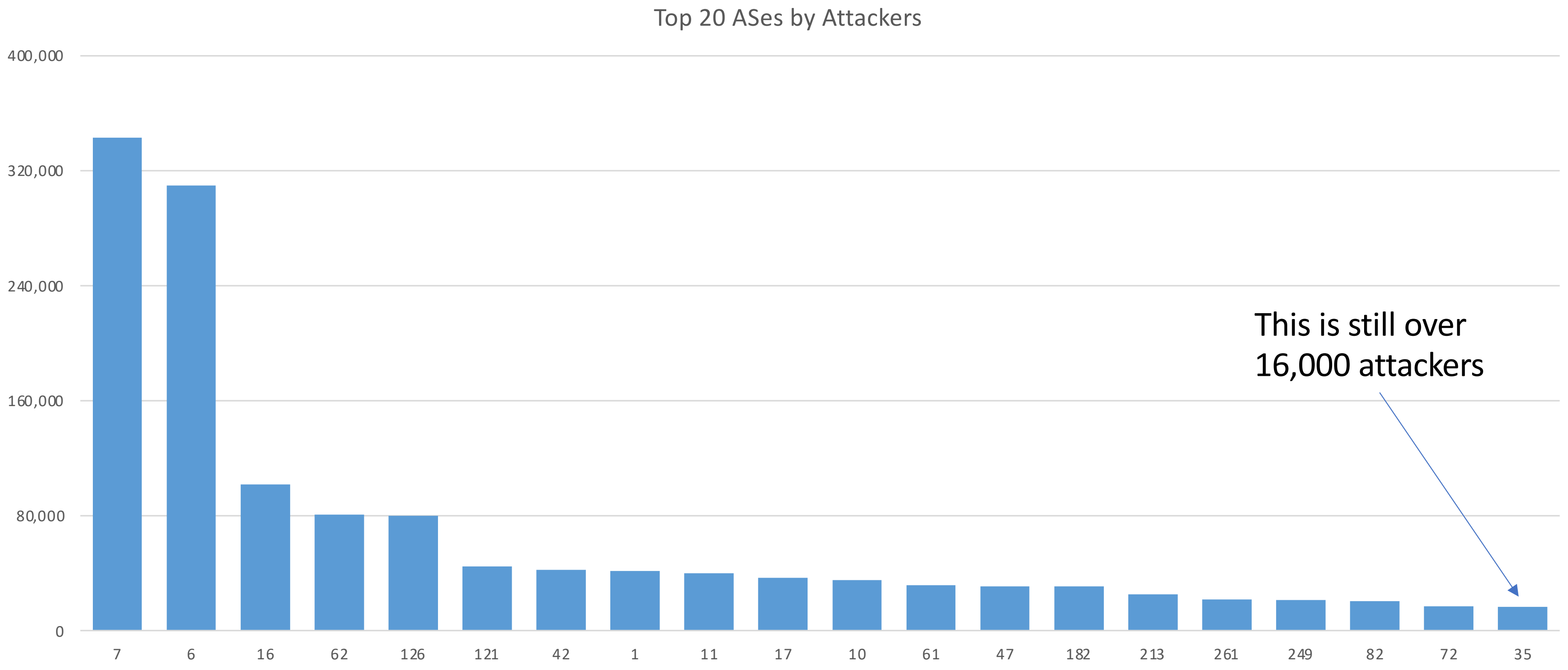
- Our ~200 sensors saw attacks from
  - 18,869 ASes
    - 4,558 of them fielded more than 1,000 attacks on our sensors
    - 212 of them launched attacks from more than 1,000 distinct IP addresses
  - 2,460,475 distinct IP addresses

Numbers of attacks



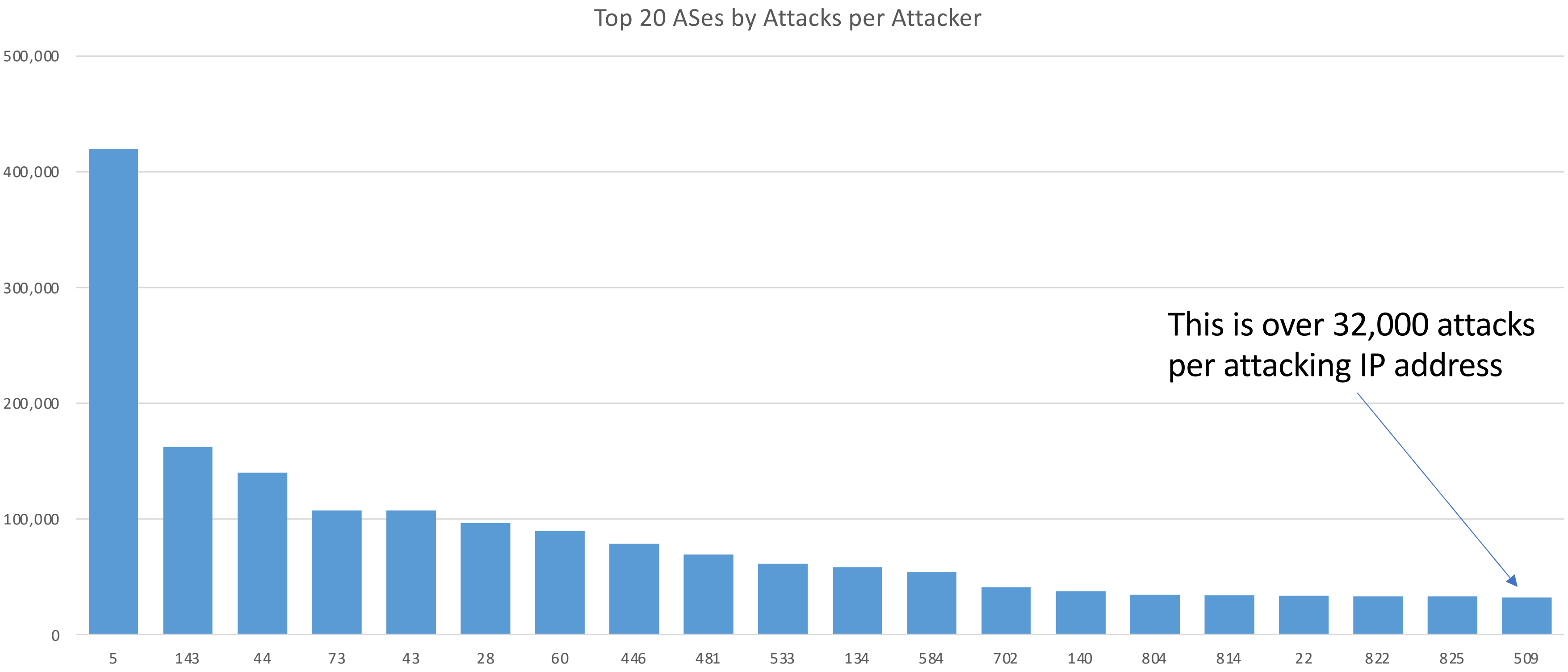
This is still over 3.3M attacks

Number of Attackers



This is still over 16,000 attackers

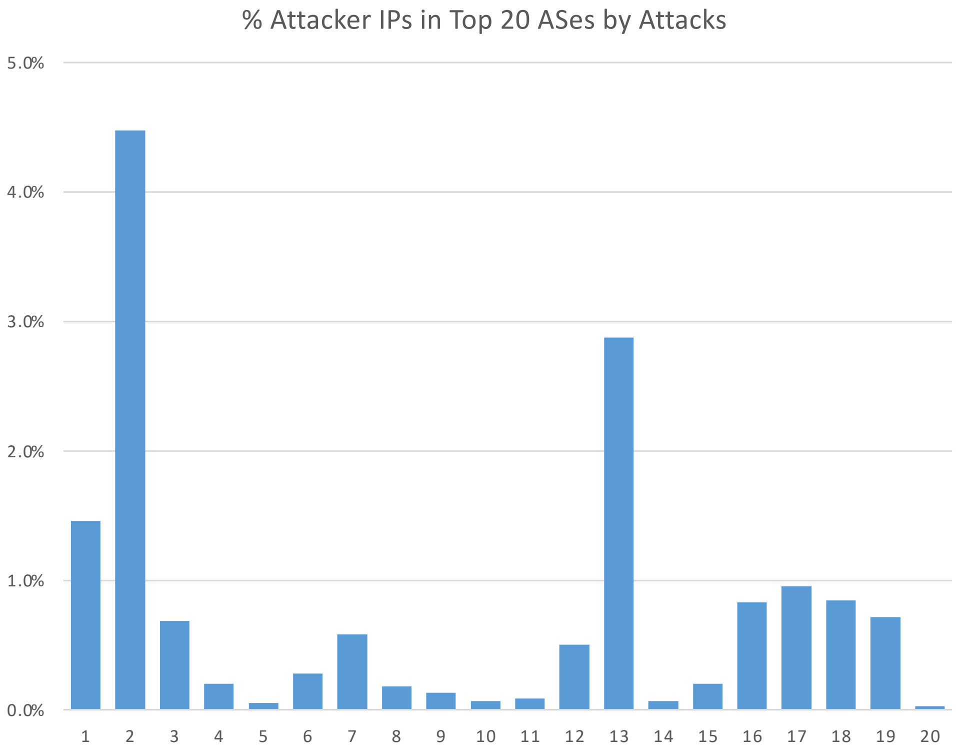
Activity of Attackers

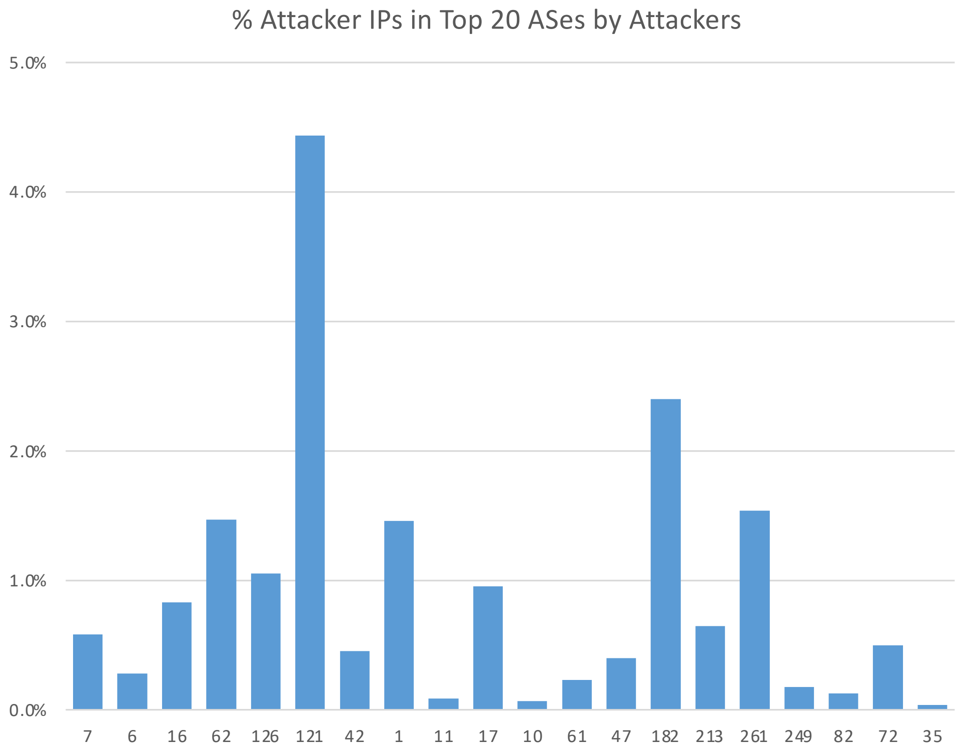


This is over 32,000 attacks per attacking IP address

Percentage of bad actors in a network

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


% Attacker IPs in Top 20 ASes by Attacks


% Attacker IPs in Top 20 ASes by Attackers

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 behavior is small (less than 5% 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
- To join us with a small group of network operators (3-5) who are interested in working together to combat this problem

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? proberts @ globalcyberalliance.org