Oh, what a crazy month it's been

What do we provide?

- DefCon, DefCon-WPA3 and DefCon-Open Wireless
  - for general Internet and conf activities
- Support DEF CON Departments
  - e.g. DCTV talk streaming
- Special requests from the floor
  - contest servers

This has been a little different...
For a variety of reasons,
We really only had 28 days of hard planning

Fastest opening for Wi-Fi and Wi-Fi Reg
Fastest completion of the drops
Most miles walked

What did setup look like

Sunday
Load in, Core and Switches

Monday
Work with Cox setting up patches
Start Wi-Fi setup

Tuesday
Stand Up DefCon
DefCon-Open
Wi-Fi Reg

Wednesday
Drops
Drops
Drops

Thursday
A few more Drops and Defcon-WPA3

Sleep

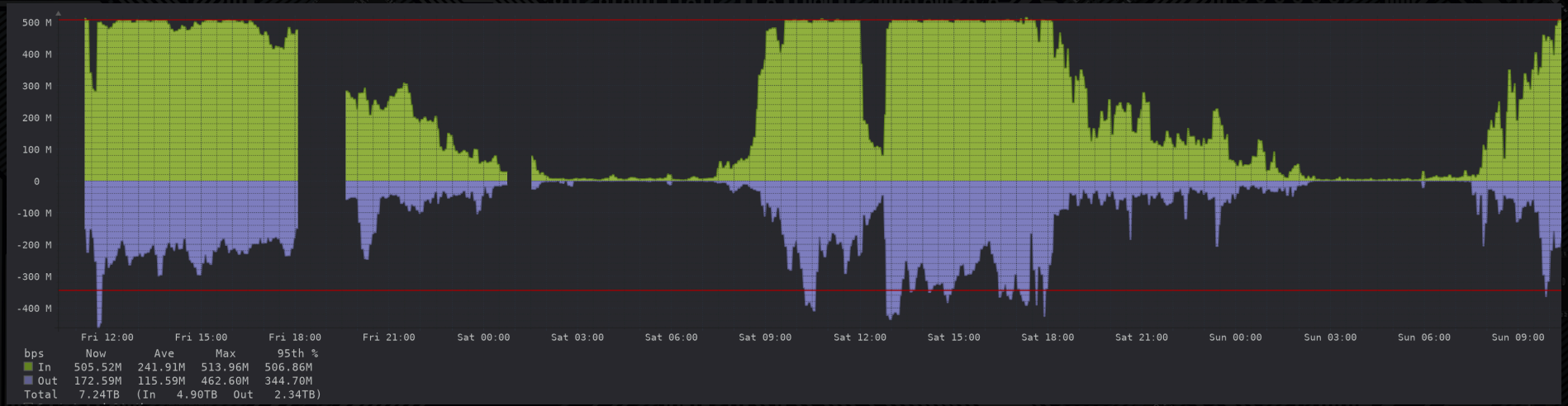
~~Sleep~~
Network Brain Surgery

Sunday
Take it all down and go home

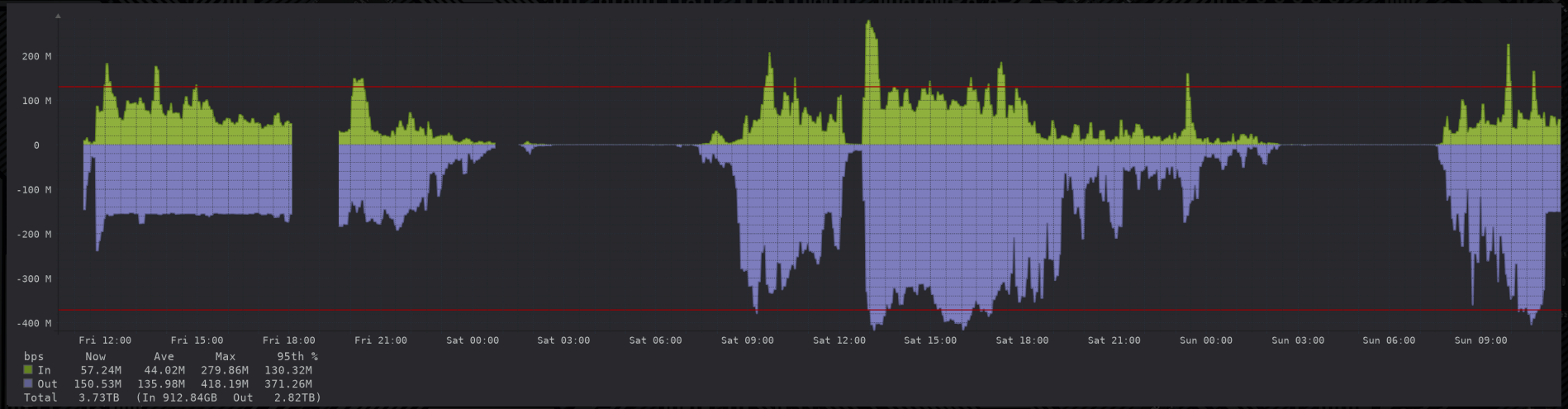
The Gear List

- ~~1~~2 FreeBSD Firewall(s)
- 1 Core Switch (3172PQ - "new")
- 650 Access Points via the Cox Wireless Network
- 32 Edge Access Switches (up 10 from previous year)
  - 100 floor drops (~what we had previously)
- 2 Servers - radius, monitoring
- The DEF CON Media Server

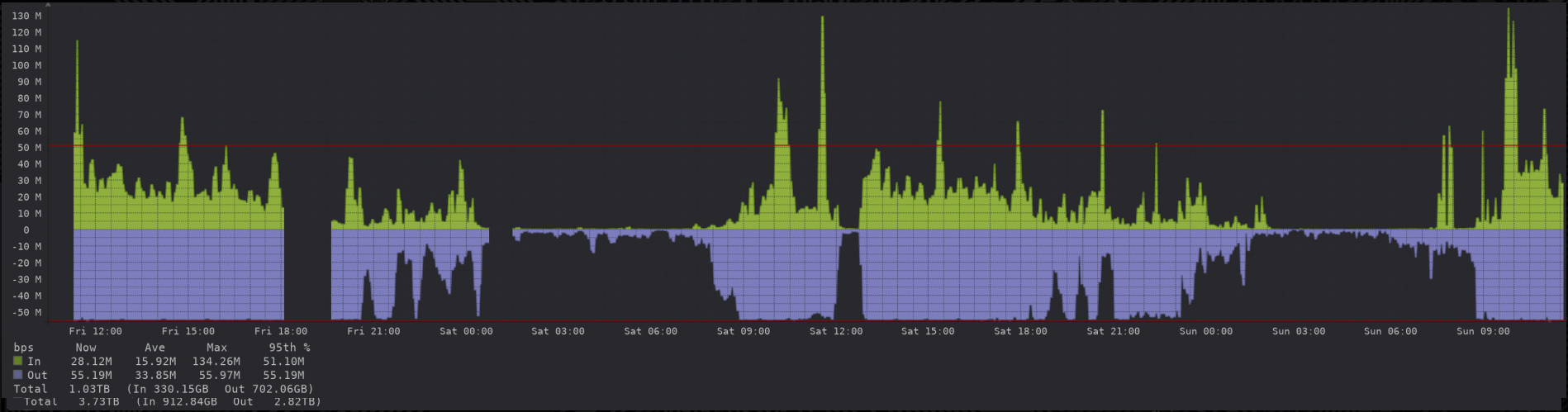
Internet Bandwidth



DefCon Secure (DefCon + DefCon-WPA3)



DefCon-Open


130 M
120 M
110 M
100 M
90 M
80 M
70 M
60 M
50 M
40 M
30 M
20 M
10 M
0
-10 M
-20 M
-30 M
-40 M
-50 M
Fri 12:00
Fri 15:00
Fri 18:00
Fri 21:00
Sat 00:00
Sat 03:00
Sat 06:00
Sat 09:00
Sat 12:00
Sat 15:00
Sat 18:00
Sat 21:00
Sun 00:00
Sun 03:00
Sun 06:00
Sun 09:00
bps Now Ave Max 95th %
In 28.12M 15.92M 134.26M 51.10M
Out 55.19M 33.85M 55.97M 55.19M
Total 1.03TB (In 330.15GB Out 702.06GB)
Total 3.73TB (In 912.84GB Out 2.82TB)

Wireless Clients

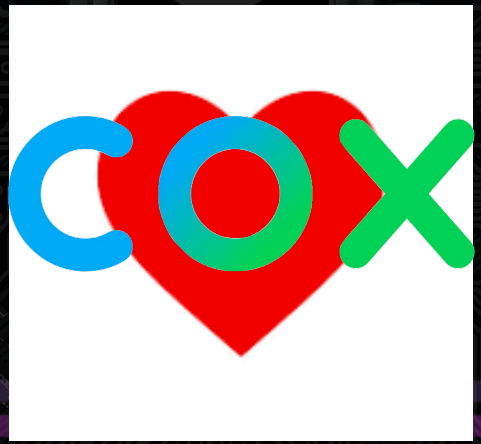
65% Secure
35% Open

Challenges

- “OMG THESE PEOPLE ARE HEATHENS”….Defcon NOC monitoring network usage
- “They just cant get enough” ….. NOC monitoring
- Friday Morning outage…. Nothing like hitting the peak right out of the gate and then slamming on the breaks…..stop forwarding your self… stop forwarding your self.
- Saturday DHCP server hangover

Wireless

- Bit of a different setup with DefCon using the internal Wi-Fi setup and Cox assisting.
  Same awesome DefCon-Open and DefCon (and DefCon-WPA3) just way more gear.



Internet

- Bandwidth is a struggle every year and while we would love to have infinite bandwidth, we do the best we can with what we have.

WIFI Extras

- 989 = Number of unique SSID's advertised around the NOC
- 38 = Number of unique Pwnagotchis detected around the NOC
- 382 = Number of Frames detected from Pineapple devices
- 31 = Number of De-authentication flood attacks detected around the NOC
- 15 = Number of attempts to spoof any of DefCon SSIDs

Most advertised unknown networks

- TMobileWingman
- pwned
- big turd
- Council of Ricks
- openwireless.org2
- 0D4YMYD3C0
- HackMyHat
- Searching...
- Dr_Dr0n3-GuessMyPassword
- SwapSpot
- Pineapple_2E49
- Avalon
- Guppy
- MSG_Guest
- SQUEEZE

Alert Report from our Cox Communications Partner

We're committed to maintaining a strong, secure network. We're happy you all had a positive experience in Las Vegas. As requested, here is the DEF CON security threat monitoring information you requested.

Alert Breakdown:
- Friday: 274
- Saturday: 1,338
- Sunday: 215

Incidents:
- Incident involving a system conducting mass internet-wide port scanning.
- Incident involving a system with various internet-exposed ports

Observables:
- One observation of a system infected with SectopRAT/Arechclient2
- Multiple instances regarding downloads of cryptocurrency miners and various backdoor payloads
- Multiple instances of external web hosting scanning using custom tools, DirBuster, Nmap, etc.
- Several instances of downloads/updates involving Metasploit, Kali Linux, and other [post-]exploitation frameworks
- Several instances of malicious python, PowerShell, and other files observed
- Multiple instance of victim and C2 side of BYOB (Bring Your Own Botnet)
- Multiple instances of connections and DNS for crimeware hosts, including spam redirects, fake update downloads, etc.
- Multiple instances of connections or DNS associated with various malware tooling such as BEEF, HAVOC, CobaltStrike, GOST, and more.
- DNS queries for known APT hostnames observed.

Thanks

DT
Janet
Nikita
Mo and GAG LAB
Department Leads
QM
Cox
LVCVA
Every other DEF CON Goon
YOU!

The NOC Team

- Leads
  - #sparky
  - mac
- Chief of Staff
  - effffn
- Infra/Systems
  - MikeD
  - c7five
  - booger
  - deadication
  - dp1i
- Monitoring
  - c0mmiebstrd
- Wi-Fi
  - CRV
  - Jon2
- Runners
  - wish
  - strange
  - Toph
  - k4tn155
  - duffguy
  - tater
  - meiBo
  - Johntitor