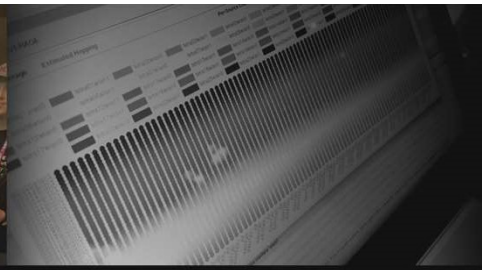
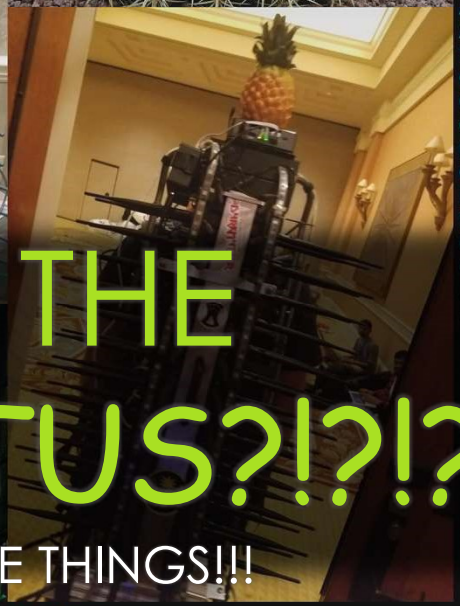




WHAT THE #WIFICACTUS?!?!?!11

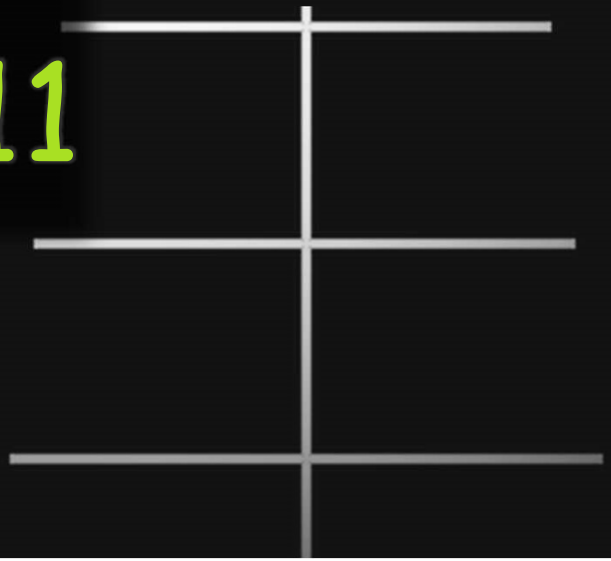
MONITOR ALL THE THINGS!!!

```
Adjusting Wireless Fidelity.................Done!
Aligning TCP Steam..................Done!
Searching for incoming socket...................Done!
Connecting 802.11a...............Done!
Connecting 802.11b.............................Done!
Connecting 802.11c-z...............................Done!
Netcatting incoming to outgoing socket......Done!
Computing vectors to Kismet instance.....Done!
Loading WiFi Cactus parameters.................Done!
Starting WiFi Cactus................Done!
Configuring all known channels.............Done!
Capturing all the WiFi things.............In Progress...
.....................In Progress.........................
.....................In Progress.........................
```

```
d4rkm4tter:
        RT @d4rth: Just hanging out with the
        #wificactus while working on
        #dcdarknet badge @d4rkm4tter
        @defcon https://t.co/qBZxATKF2H
        2017-07-29 05:20:16

d4rkm4tter:
        RT @steve0: @d4rkm4tter When and where
        can I feel up the #wificactus?
        2017-07-29 06:17:14

d4rkm4tter:
        @urmom @b3nderb4dge Wait didn't you
        get the message that the #wificactus
        is a lie?
        2017-07-29 06:25:02
```



#ME

Source: CNET Article https://goo.gl/5w6diu

- I wear the #wificactus
- I play a hacker in the cyber sphere
- I can program
- I can computate
- Freelance Infosec
  - Hit me up if interested!
- BS in Computer Science

HUGE THANK YOU TO SOOO MANY PEOPLE WHO MADE THIS POSSIBLE!!!!

- Hak5 (Darren, Seb, Shannon, Jayson, Sarah, and everyone else)
- BH (Grifter, Stumper, L34n, Nemus, Cesar, and everyone else I'm forgetting)
- DefCon (DT, Kampf, Jeremy, SOC Goons, and everyone else I'm forgetting)
- Renderman, Sid and the DC Wireless Village
- Luxor and Mandalay security
- Austin, Bryan, Henry

- AND ESPECIALLY ALL OF YOU!!!!!!!!!!!!!

#WHY MONITOR WIFI?

- It's everywhere, everyone uses it and nearly every device has it
- People make assumptions about security and trust vendors/hardware blindly
- To better understand risks
- To detect the risks
- To monitor for threats
- Stuff worth finding
- Curiosity

#PROJECT HISTORY: DEFCON23 WARWALKER

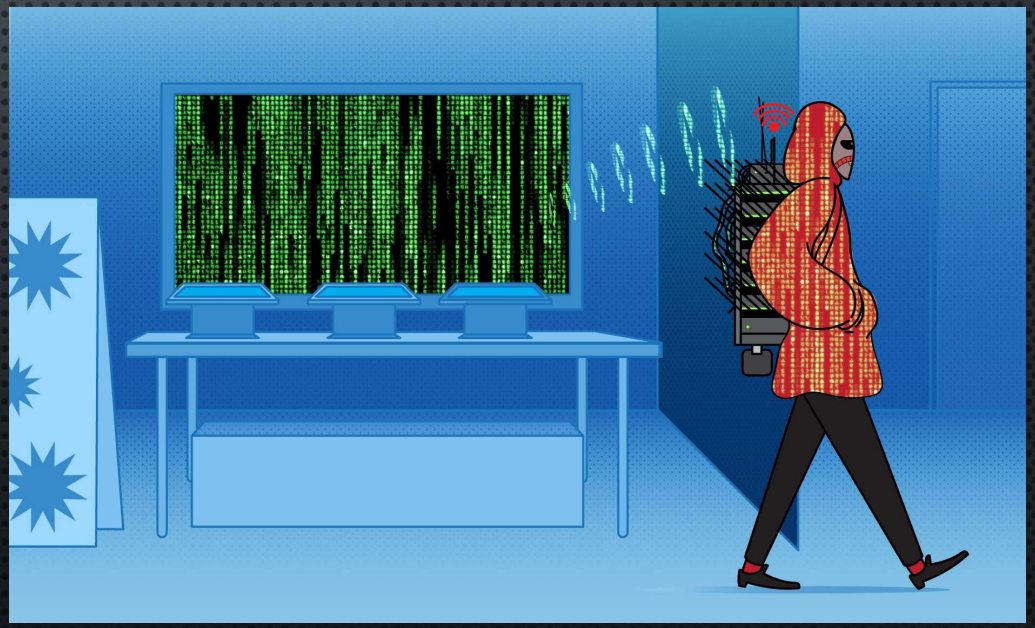
- Beaglebone Black
- 2 Alfa radios
- 12 hours of battery life
- Super interesting stuff
- Saintcon talk is online somewhere
- Used aircrack-ng framework
- Inspired me to do more

#PROJECT HISTORY: PROJECT LANA

- Took lessons learned from previous year
- Got sponsored by Minnowboard (Intel)
- Deployed 2 boxes at BH and 12 at DefCon
- Learned about Kismet
- Saintcon talk online somewhere

THE #WIFICACTUS: BACKGROUND

- Wanted to do something bigger than last year
- Grifter made me go to Shmoocon
- Met with Darren Kitchen (Hak5)
- HAK5 totally hooked it up!!! #sponsored!!!!



Source: CNET Article https://goo.gl/5w6diu

#SPONSORED

- Things got real, 40 Hak5 Tetra pineapples showed up
- Support https://hakshop.com

THE #MINI-CACTI

- Proof of concept
- 6 HAK5 Pineapple Tetras
- 25 AH Battery
- Minnowboard

THE #WIFICACTUS: THE BUILD

- Hardware:
  - 25 HAK5 Pineapple Tetras
    - 50 ATH9 Radios
    - 100 Antennas (2x2 MIMO)
  - 2 Cisco 16 port 10/100 Switches
  - Intel NUC i5 16GB Ram 512GB SSD
  - 500 Watt 12v PSU
  - Arduino Micro
  - A lot of LEDs
  - Lead Acid Small Car Battery

THE #WIFICACTUS: THE BUILD

THE #WIFICACTUS: THE BUILD

ACCIDENTAL BEACON DDOS

- Turns out you can DDOS with only beacons
- Lesson learned: Load firmware and power on 1 at a time

18 scanned in 13871ms. DB Queue: 0

Pineapple_165B Orient Power Home Network Ltd. - 5:10:16
-68 | 00:13:37:a6:16:5b - 11 - [ESS]

Pineapple_167B Orient Power Home Network Ltd. - 5:10:16
-72 | 00:13:37:a6:16:7b - 11 - [ESS]

Pineapple_128F Orient Power Home Network Ltd. - 5:10:16
-73 | 00:13:37:a6:12:8f - 11 - [ESS]

Pineapple_1673 Orient Power Home Network Ltd. - 5:10:16
-75 | 00:13:37:a6:16:73 - 11 - [ESS]

Pineapple_164C Orient Power Home Network Ltd. - 5:10:16
-75 | 00:13:37:a6:16:4c - 11 - [ESS]

Pineapple_1664 Orient Power Home Network Ltd. - 5:10:16
-75 | 00:13:37:a6:16:64 - 11 - [ESS]

Pineapple_1640 Orient Power Home Network Ltd. - 5:10:16
-75 | 00:13:37:a6:16:40 - 11 - [ESS]

Pineapple_1290 Orient Power Home Network Ltd. - 5:10:16
-78 | 00:13:37:a6:12:90 - 11 - [ESS]

Pineapple_168B Orient Power Home Network Ltd. - 5:10:30
-79 | 00:13:37:a6:16:8b - 11 - [ESS]

Pineapple_1693 Orient Power Home Network Ltd. - 5:10:30
-80 | 00:13:37:a6:16:93 - 11 - [ESS]

Pineapple_1667-5G Orient Power Home Network Ltd. - 5:10
-91 | 00:13:37:a6:16:68 - 36 - [ESS]

Pineapple_1690 Orient Power Home Network Ltd. - 5:10:30
-91 | 00:13:37:a6:16:90 - 11 - [ESS]

THE #WIFICACTUS: THE FRAME

- Custom aluminum top and bottom plate
- Custom Delrin rails to support alternating direction
- Handle
- Open frame backpack

- THANK YOU AUSTIN AND BRYAN!!!!

THE #WIFICACTUS: THE PINEAPPLE

- Met Richard at Blackhat
- He bought a Pineapple on amazon and had it overnighted to a locker on the strip
- Iconic addition to the project

- It takes a community to make this stuff happen!

THE #WIFICACTUS: SOFTWARE

- Default Tetra firmware, because lazy
  - Default tetras beacon DDOS
- Kismet on the NUC
- Kismet Remote Client on the 25 Tettras
- Ansible and very bad bash scripts to manage everything
- Organic, hand flashed Pineapple tetras by Bryan and Henry
- Everyhing goes to in a single Kismet session and single PCAP file

Kismet Wireless

- Support Kismet on Patreon:
- http://goo.gl/yX3RJT

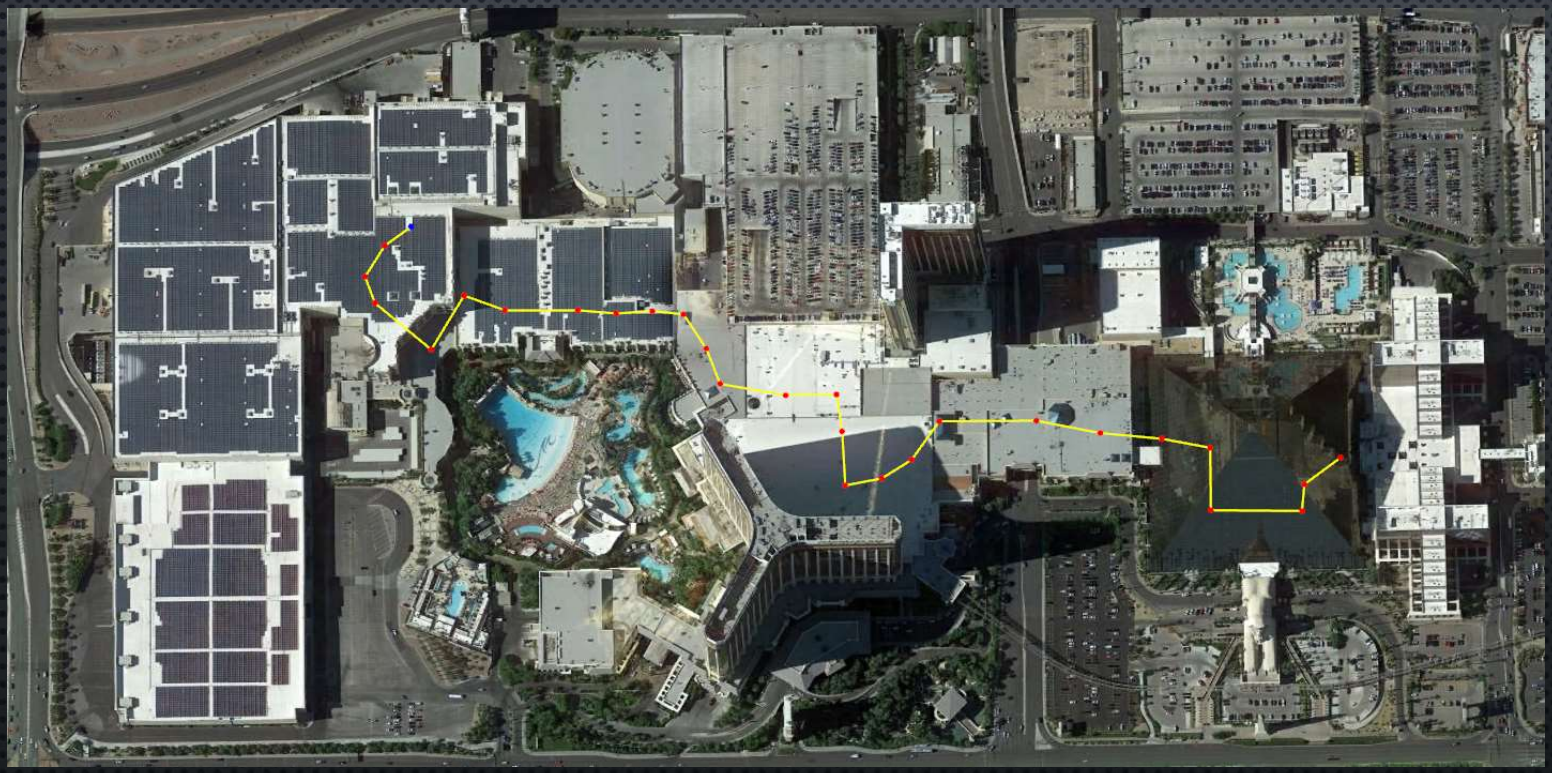
THE #WIFICACTUS: FAQ

- How much does it weigh, is it heavy?
- How much data does it get?
- Are you getting cancer?
- Are you planning on having kids?
- Is it hot?

THE #WIFICACTUS: FAQ

- How much did it cost?
- How much time did it take to make?
- What did TSA think about it?
- How long does it last on battery?

MY WARWALK



- 4,274 FEET
- ~1,800 STEPS
- 14,805 TOTAL STEPS THAT DAY
- POWER STEPS!

THE #WIFICACTUS: THE BLACKHAT NOC

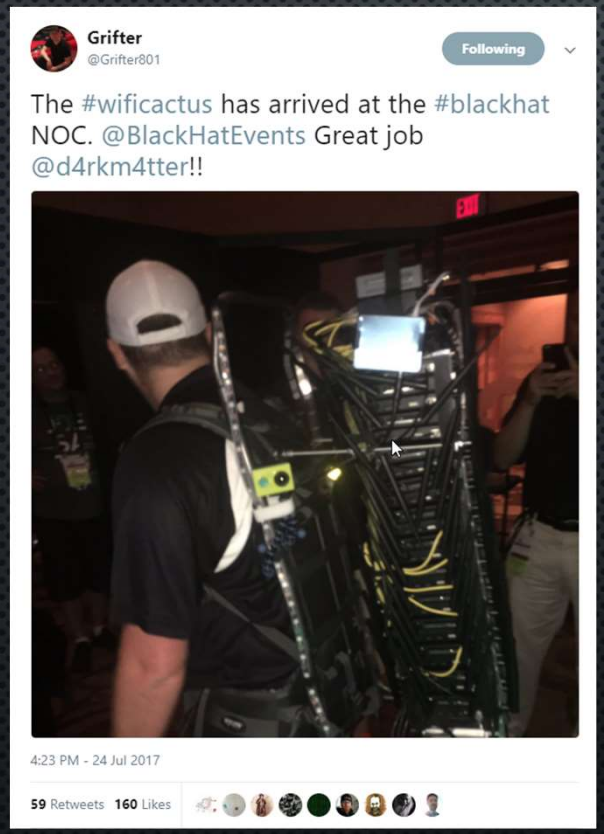


Photo Credit: PCMag

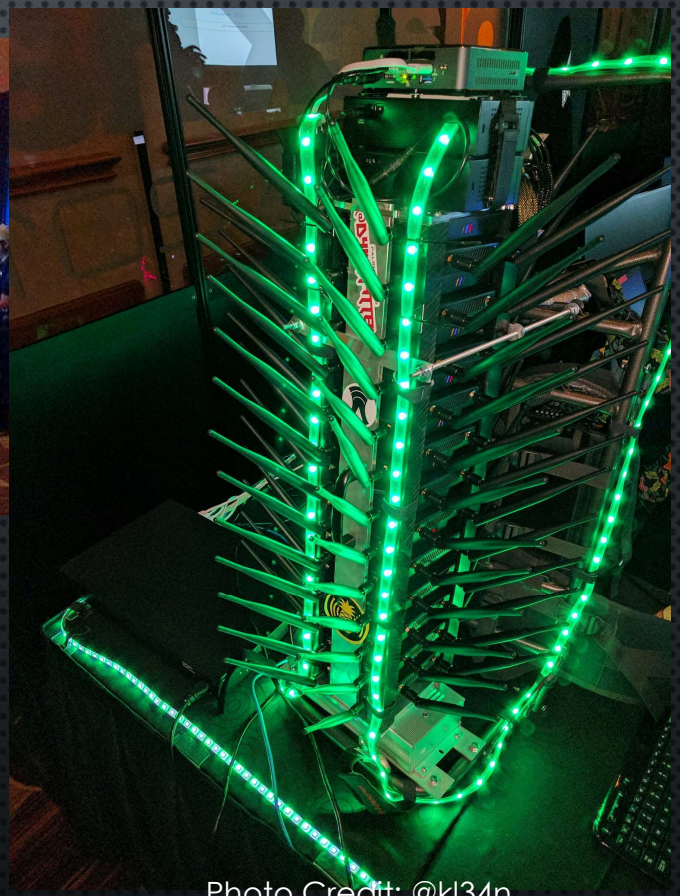


Photo Credit: @kl34n

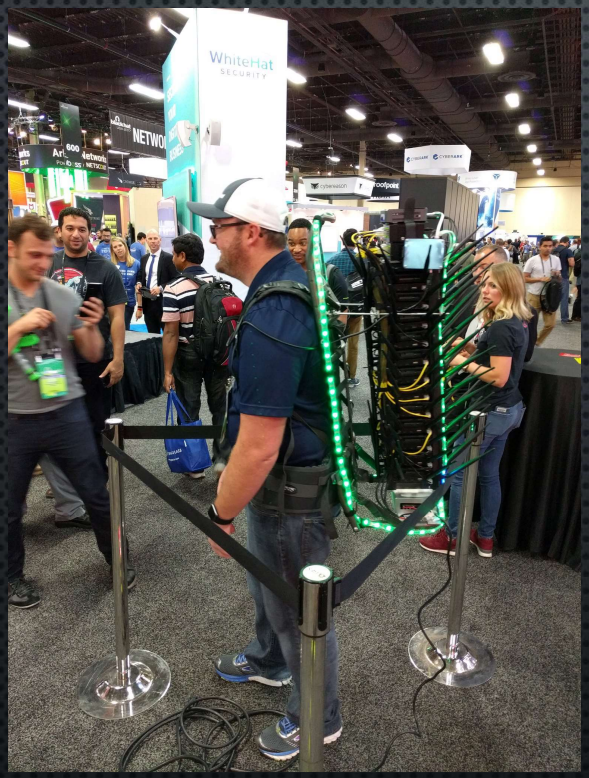
THE #WIFICACTUS: THE BLACKHAT NOC

"Can I haz the WiFi?"

Photo Credit: @kl34n

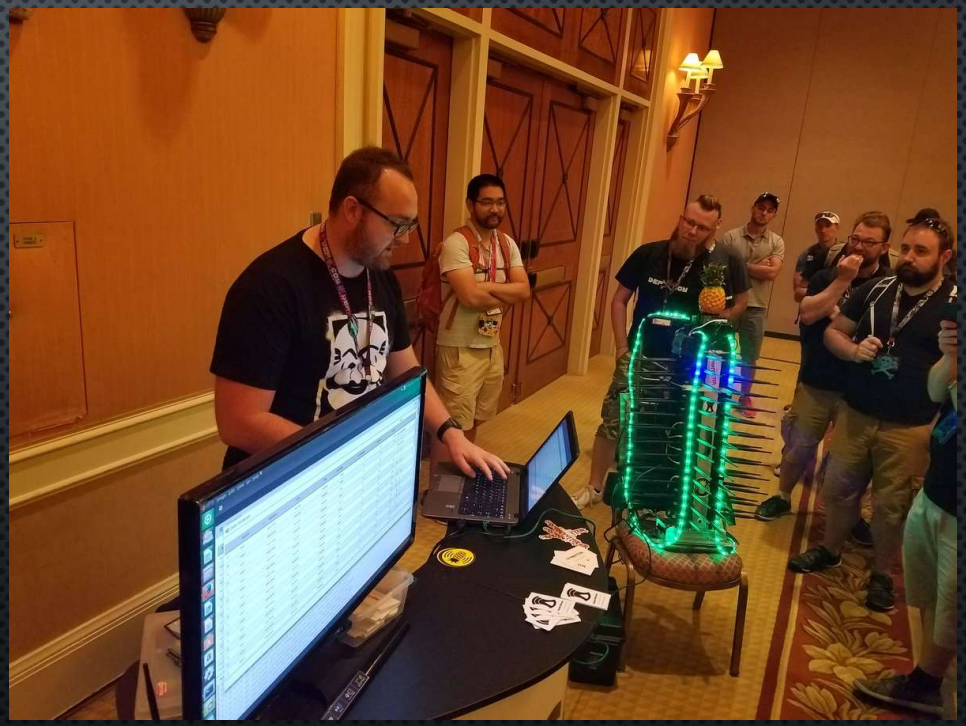
THE THING ABOUT THE LUXOR….

THE #WIFICACTUS: VISITING BH VENDORS



THE #WIFICACTUS: LOCATION DEFCON

THE #WIFICACTUS: DEMOLABS



THE #WIFICACTUS: CACTUSCON

THE DATAS

PREPARING FOR THE WIFI DROUGHT

	2017	2016	2015
Total Captured PCAP Size	138 GB	42 GB	280 MB
Total Unique Mac Address	104 thousand	253 thousand	A few thousand
Total Unique SSIDs	309 thousand	237 thousand	A few hundred

SHOW ME THE DATA

Location	Capture Time	Size
Blackhat NOC	3 days	65 GB
Blackhat Vendors	60 Min	4 GB
Blackhat WarWalk	30 Min	3 GB
DefCon Warwalk	7 Hours	18 GB
DefCon Demolab	5 Hours	45 GB
CactusCon	6 Hours	3 GB

Kismet-20170725-19-04-28-1.pcapdump	1,227,104 KB	PCAPDUMP File
Kismet-20170726-10-24-30-1.pcapdump	477,533 KB	PCAPDUMP File
Kismet-20170726-14-17-38-1.pcapdump	554,628 KB	PCAPDUMP File
Kismet-20170726-15-46-24-1.pcapdump	11,170 KB	PCAPDUMP File
Kismet-20170726-16-10-47-1.pcapdump	0 KB	PCAPDUMP File
Kismet-20170726-16-12-39-1.pcapdump	18,126 KB	PCAPDUMP File
Kismet-20170726-16-38-37-1.pcapdump	33,371 KB	PCAPDUMP File
Kismet-20170726-17-06-28-1.pcapdump	5,455,707 KB	PCAPDUMP File
Kismet-20170729-08-51-39-1.pcapdump	991,168 KB	PCAPDUMP File
Kismet-20170729-09-34-11-1.pcapdump	1,175,072 KB	PCAPDUMP File
Kismet-20170729-10-09-57-1.pcapdump	44,894 KB	PCAPDUMP File
Kismet-20170729-10-15-07-1.pcapdump	244 KB	PCAPDUMP File
Kismet-20170729-10-16-44-1.pcapdump	2,911,984 KB	PCAPDUMP File
Kismet-20170729-11-53-29-1.pcapdump	426,224 KB	PCAPDUMP File
Kismet-20170729-12-04-16-1.pcapdump	932,848 KB	PCAPDUMP File
Kismet-20170729-12-28-21-1.pcapdump	2,311,400 KB	PCAPDUMP File
Kismet-20170729-13-27-10-1.pcapdump	2,454,546 KB	PCAPDUMP File
Kismet-20170729-13-52-11-1.pcapdump	1,808,574 KB	PCAPDUMP File

MAC ADDRESS SUMMARY

	Count
Total Unique Source Addresses (SA)	104,023
Total Unique Destination Addresses (DA)	96,133
Total Unique Receiver Addresses (RA)	104,151
Total Unique Mac Addresses	104,084

MOST NOISY AP'S TOP 20

SSID	COUNT
CaesarsVillas	8,807,235
CAESARS	8,714,551
BETA	6,075,116
ALPHA	6,051,288
DefCon-Open	2,996,732
DefCon	2,899,050
Caesars_Resorts	2,768,050
DELTA	2,039,118
GAMMA	2,025,671
BlackHatUSA2017	1,827,242

SSID	COUNT
MGMResorts-WiFi	1,269,576
CDOBM	1,196,461
MPTS	1,184,613
MMD	1,180,436
Sca2	568,035
Verizon-291LVW-3DB3	518,463
PirateBox - Share Freely	394,499
AMX	345,149
T-Mobile Broadband19	280,779

THE FREQUENCIES (MHZ)

CHAN	CHAN	CHAN	CHAN
2412	2417	2422	2427
2432	2437	2442	2447
2452	2457	2462	5180
5200	5220	5240	5260
5280	5300	5320	5500
5520	5540	5560	5580
5600	5620	5640	5660
5680	5700	5745	5765
5785	5805	5825	

- 40 TOTAL CHANNELS MONITORED

THE ALERTS

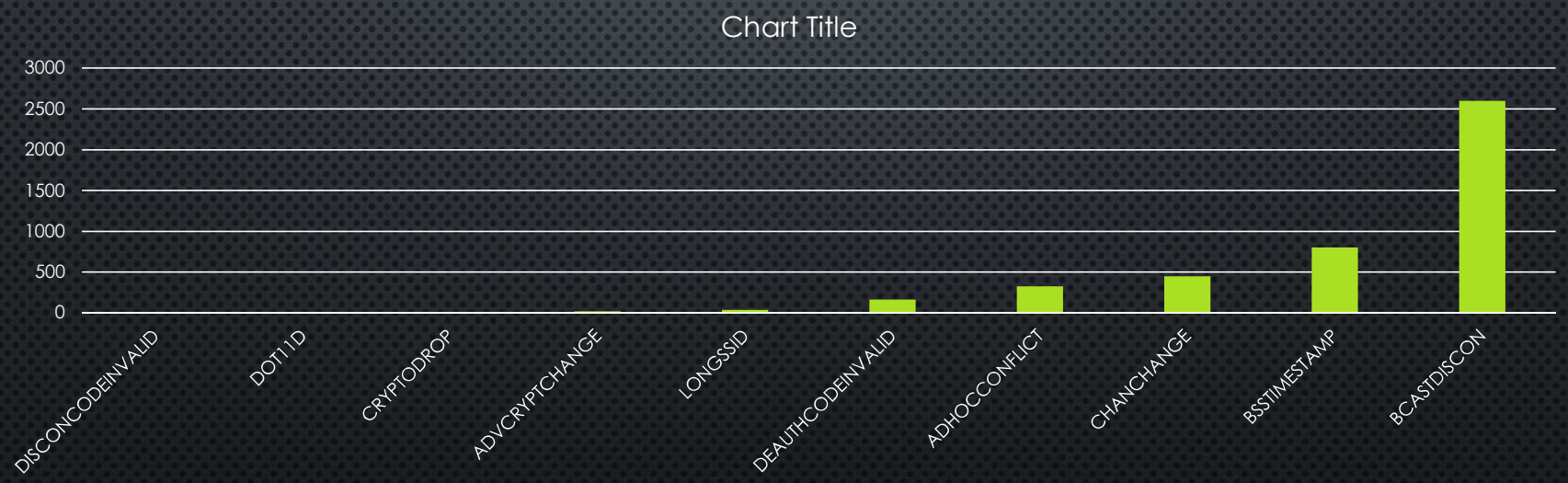


Chart Title
3000
2500
2000
1500
1000
500
0
DISCONCODEINVALID
DOT11D
CRYPTODROP
ADVCRYPTCHANGE
LONGSSID
DEAUTHCODEINVALID
ADHOCCONFLICT
CHANCHANGE
BSSTIMESTAMP
BCASTDISCON

INTERESTING EVENTS

SSID	EVENT
Configure.Me-097930	changed advertised encryption from none to WPA WPA-PSK AES-CCMP which may indicate AP spoofing/impersonation
	changed advertised encryption from WPA WPA-PSK AES-CCMP to WEP which may indicate AP spoofing/impersonation
	changed advertised encryption from WEP to WPA WPA-PSK AES-CCMP which may indicate AP spoofing/impersonation
sca2	changed advertised encryption from WPA AES-CCMP to WPA WPA-PSK AES-CCMP which may indicate AP spoofing/impersonation
DefCon	changed advertised encryption from WPA AES-CCMP to WPA WPA-PSK AES-CCMP which may indicate AP spoofing/impersonation
DefCon	changed advertised encryption from WPA WPA-PSK AES-CCMP to WPA AES-CCMP which may indicate AP spoofing/impersonation
OutboxScanners	changed advertised encryption from WPA WPA-PSK AES-CCMP to WPA AES-CCMP which may indicate AP spoofing/impersonation
360WiFi-7E6F9A-5G	changed advertised encryption from WPA WPA-PSK AES-CCMP to WPA WPA-PSK TKIP AES-CCMP which may indicate AP spoofing/impersonation
360WiFi-7E6F9A-5G	changed advertised encryption from WPA WPA-PSK TKIP AES-CCMP to WPA WPA-PSK AES-CCMP which may indicate AP spoofing/impersonation
WCTF_06	changed advertised encryption from none to WEP which may indicate AP spoofing/impersonation

BROADPWN

975…	32.970922	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=33, FN=0, Flags=.....C, BI=15, SSID=broadpwn_test[Malformed… 802.11b
975…	32.974648	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=33, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malformed… 802.11b
975…	32.981137	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=33, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malformed… 802.11b
975…	32.984135	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=33, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malformed… 802.11b
975…	33.001317	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=33, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malformed… 802.11b
975…	33.004520	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=33, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malformed… 802.11b
975…	33.009975	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=33, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malformed… 802.11b
268…	83.258614	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=490, FN=0, Flags=.....C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
268…	83.260304	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=490, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
350…	109.646219	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=718, FN=0, Flags=.....C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
350…	109.648734	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=718, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
350…	109.655216	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=719, FN=0, Flags=.....C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
350…	109.656323	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=719, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
350…	109.657426	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=719, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
350…	109.664499	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=719, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
350…	109.665743	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=719, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
350…	109.666808	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=719, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
350…	109.668155	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=719, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
410…	126.773385	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=860, FN=0, Flags=.....C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
410…	126.800071	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=861, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
410…	126.801172	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=861, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
410…	126.802957	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=861, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
410…	126.804254	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=861, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
410…	126.808996	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=861, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malforme… 802.11b
507…	152.268471	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=1035, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malform… 802.11b
507…	152.269788	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=1035, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malform… 802.11b
507…	152.271163	Alfa_84:ba:b9	Apple_d9:4a:ba	802.11	131	Probe Response, SN=1035, FN=0, Flags=....R...C, BI=15, SSID=broadpwn_test[Malform… 802.11b

```
Signal strength (dBm): -59 dBm
TSF timestamp: 3102700724
[Duration: 984 us]
  [Expert Info (Warning/Assumption): No preamble length information was available, assuming short preamble.]
      [No preamble length information was available, assuming short preamble.]
      [Severity level: Warning]
      [Group: Assumption]
```

BROADPWN

No.	Time	Source	Destination	Protocol	Length	Info
1289561	359.745863	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1974, FN=0, Flags=.....C, SSID=I AM OWNED
1289568	359.752726	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1975, FN=0, Flags=.....C, SSID=I AM OWNED
1289569	359.753419	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1976, FN=0, Flags=.....C, SSID=I AM OWNED
1289570	359.753443	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1977, FN=0, Flags=.....C, SSID=I AM OWNED
1289571	359.753469	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1978, FN=0, Flags=.....C, SSID=I AM OWNED
1289577	359.755967	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1979, FN=0, Flags=.....C, SSID=I AM OWNED
1289578	359.755994	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1980, FN=0, Flags=.....C, SSID=I AM OWNED
1289579	359.756797	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1982, FN=0, Flags=.....C, SSID=I AM OWNED
1289580	359.757499	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1983, FN=0, Flags=.....C, SSID=I AM OWNED
1289581	359.757523	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1984, FN=0, Flags=.....C, SSID=I AM OWNED
1289582	359.758166	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1985, FN=0, Flags=.....C, SSID=I AM OWNED
1289583	359.758189	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1986, FN=0, Flags=.....C, SSID=I AM OWNED
1289584	359.758551	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1987, FN=0, Flags=.....C, SSID=I AM OWNED
1289585	359.759473	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1989, FN=0, Flags=.....C, SSID=I AM OWNED
1289586	359.759500	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1990, FN=0, Flags=.....C, SSID=I AM OWNED
1289587	359.760219	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1991, FN=0, Flags=.....C, SSID=I AM OWNED
1289588	359.760240	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1992, FN=0, Flags=.....C, SSID=I AM OWNED
1289589	359.760676	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1994, FN=0, Flags=.....C, SSID=I AM OWNED
1289590	359.761378	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1995, FN=0, Flags=.....C, SSID=I AM OWNED
1289591	359.761403	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1996, FN=0, Flags=.....C, SSID=I AM OWNED
1289592	359.761421	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1997, FN=0, Flags=.....C, SSID=I AM OWNED
1289593	359.761880	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=1998, FN=0, Flags=.....C, SSID=I AM OWNED
1289605	359.769928	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=2015, FN=0, Flags=.....C, SSID=I AM OWNED
1289610	359.771253	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=2017, FN=0, Flags=.....C, SSID=I AM OWNED
1289611	359.771752	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=2018, FN=0, Flags=.....C, SSID=I AM OWNED
1289612	359.772547	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=2019, FN=0, Flags=.....C, SSID=I AM OWNED
1289613	359.772571	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=2020, FN=0, Flags=.....C, SSID=I AM OWNED
1289614	359.773768	30:07:4d:e1:5f:46	Broadcast	802.11	172	Probe Request, SN=2022, FN=0, Flags=.....C, SSID=I AM OWNED

THE #WIFICACTUS: LIVE DEMO

THE #WIFICACTUS: THE PRESS

You *could* have **one** WiFi Pineapple and hop all of the channels to capture traffic. But you *might* miss something. Better to have one for each channel.

#wificactus

THE #WIFICACTUS: THE PRESS

adafruit SHOP BLOG LEARN FORUMS VIDEOS

AUGUST 2, 2017 AT 5:00 AM

#WiFiCactus: When You Need to Know About Hackers #WearableWednesday #defcon #wearabletech #DIY

Arduino
August 2

The #WiFiCactus has a total of 50 WiFi radio that are being used for passive monitoring of nearby wireless devices.

(via Adafruit Industries)

#WiFiCactus: When You Need to Know About Hackers #WearableWednesday #defcon #wearabletech #DIY

As I was zooming through the Tweets from Defcon I came across the mac-daddy of wearables. This is the #WiFiCactus created by Mike Spicer (@d4rkm4tter), and I...

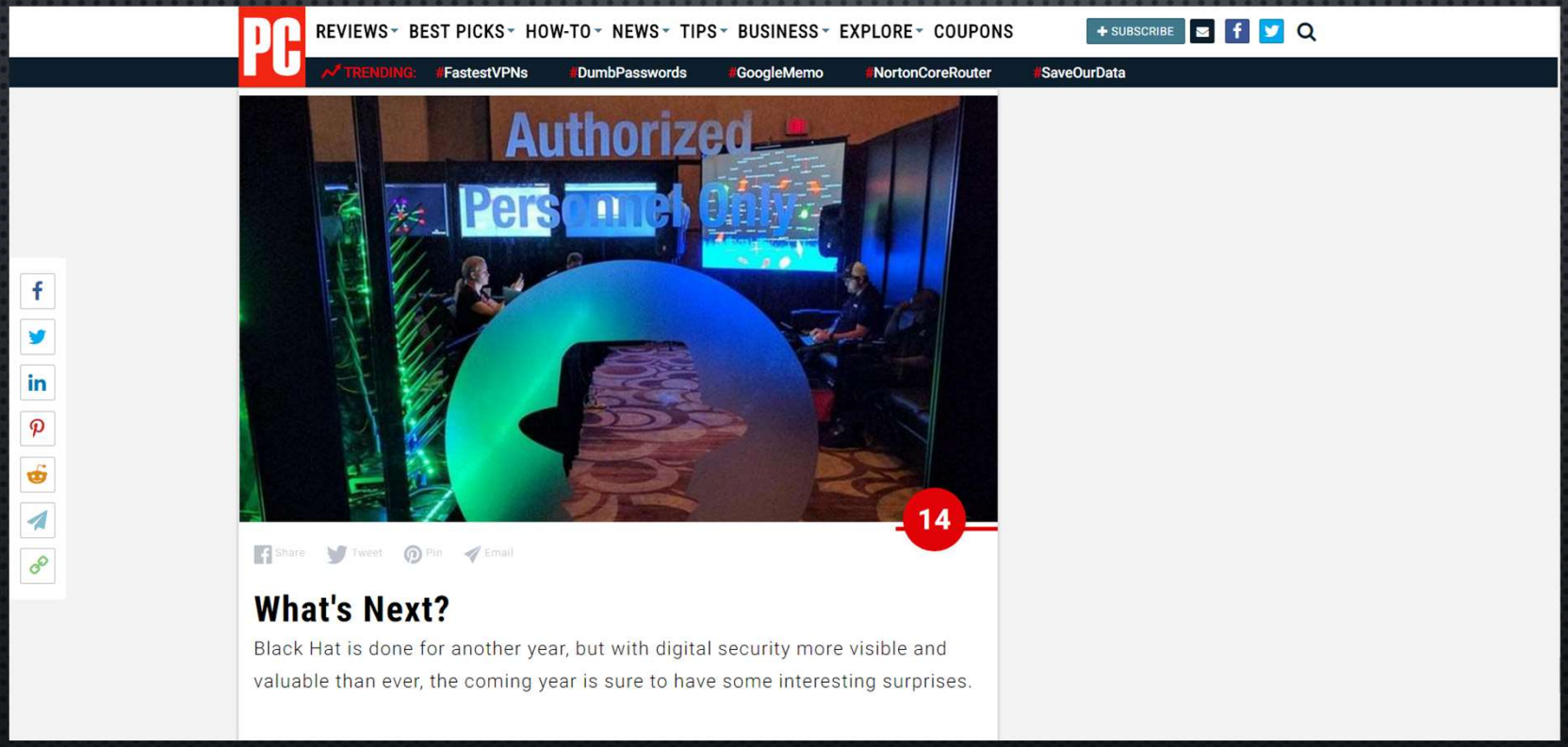
BLOG.ADAFRUIT.COM

Like Comment Share

200 Top Comments

13 Shares 2 Comments

THE #WIFICACTUS: THE PRESS



THE #WIFICACTUS: THE PRESS

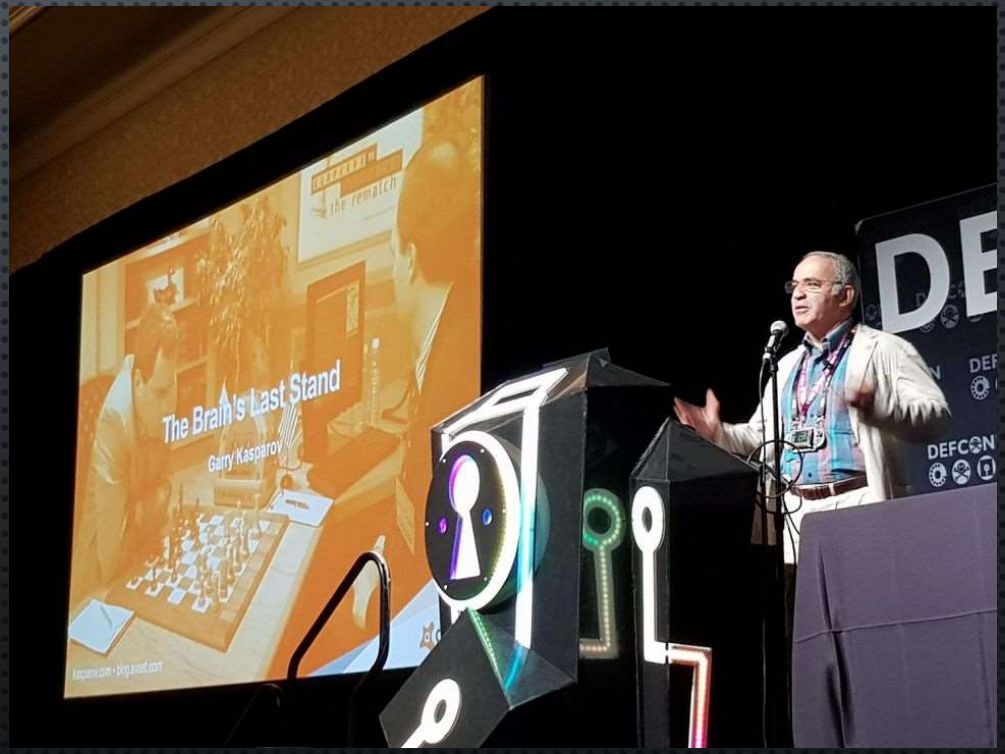
The NOC, as it's called, is a dark room only lit by screens and a spotlight that looks like Batman's Bat signal on the wall. It's a silhouette of a man in a trenchcoat and a black hat, the conference's official symbol.

In one corner is a goofy but terrifying device called a Wi-Fi cactus, that looks like a glowing tree with spiky antennas coming out. Theoretically, it can scan for thousands of connections, but these hackers mostly use it as an amusing prop.

CNET Article: https://goo.gl/qXaiEi

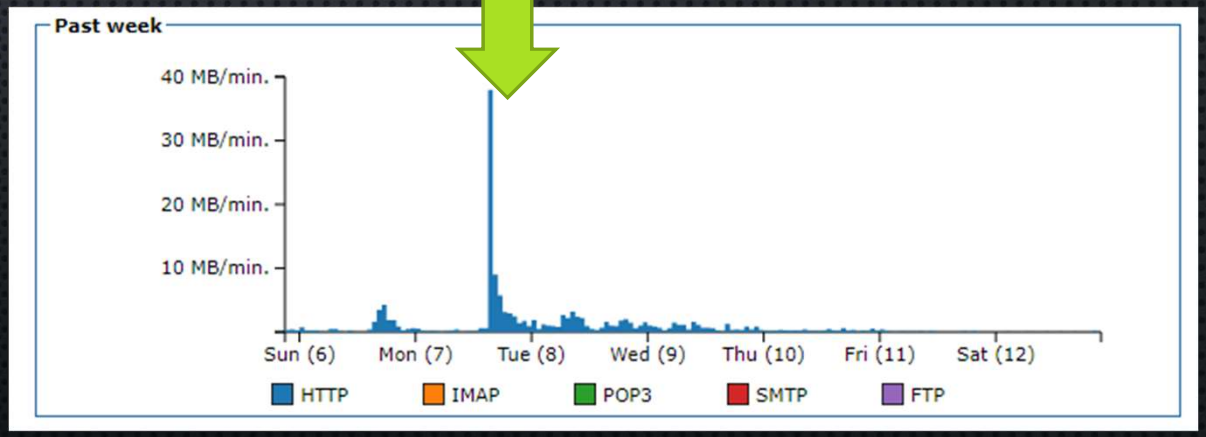
THE #WIFICACTUS: THE PRESS

- MENTIONED IN AN ARTICLE WITH SMART CITIES, AI, DAVID BRUMLEY, GARY KASPAROV
- THANKS CNET'S @ALFREDWKNG!



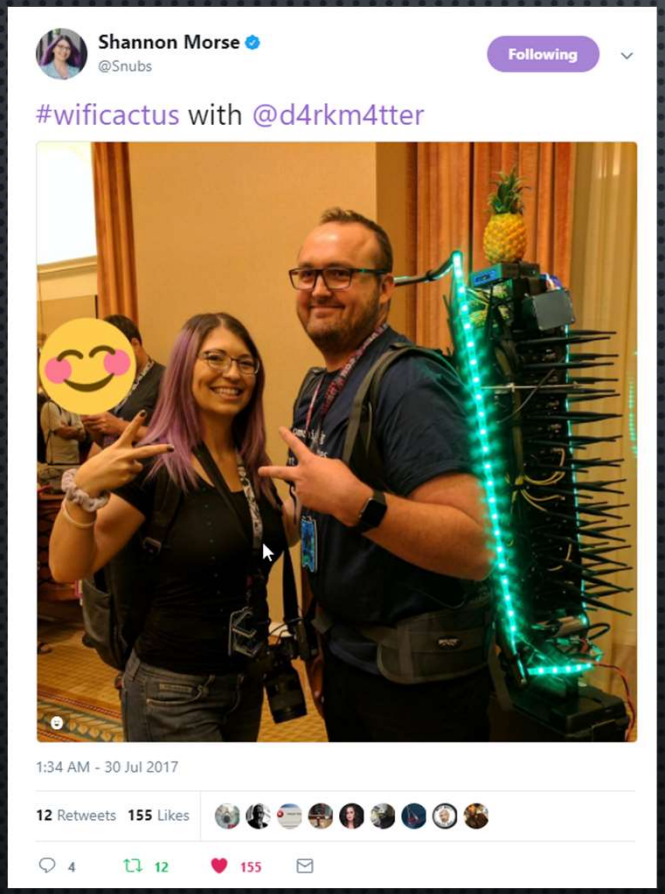
THE #WIFICACTUS: DEFCON TWEETED!!!

The Website is Down!!!!

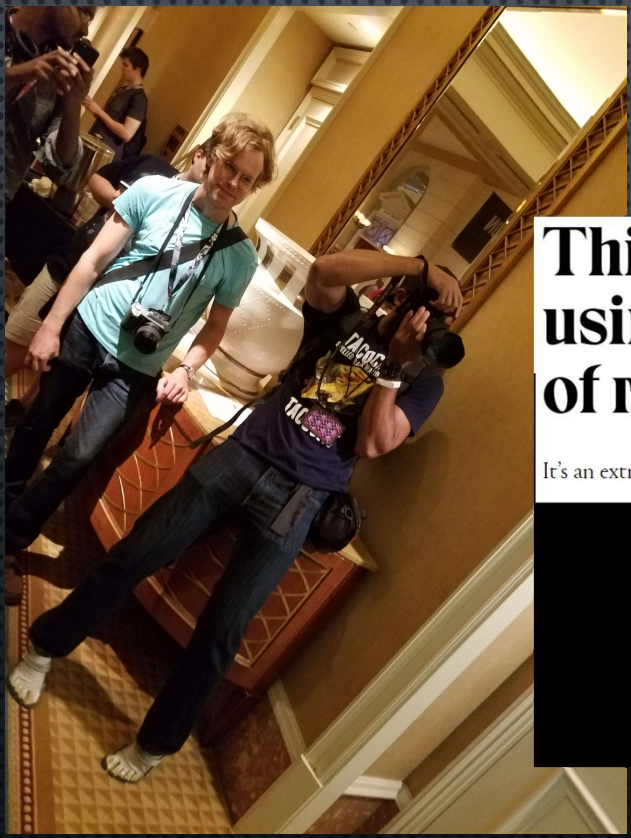


#ACHIEVEMENT: TAY!!!!

THE #WIFICACTUS: MOAR TWITTERS



THE #WIFICACTUS: INTERVIEWS



This guy hunted Wi-Fi hackers using a giant backpack made out of radios

It's an extreme version of what hackers call wardriving.

THE TWITTERS

INFOSEC @InfoSec_17 · Jul 24
Replying to @kl34n
@_sn0ww @d4rkm4tter @hak5darren 😍👌
1

Liška 🍴 🍍 @najsfoks · Jul 25
Replying to @kl34n @d4rkm4tter @hak5darren
why tho

Wesley McGrew @McGrewSecurity · Jul 24
Replying to @kl34n @d4rkm4tter and 2 others

5

Liz Henry
@lizhenry
Follow

Guy with giant wireless router backpack. Or something. Wow! #defcon

Wesley McGrew liked
🍒💀 **spookware** 💀🍒 @frootware · Aug 13
While I wasn't at DEFCON, I love talking about the #WifiCactus. My non-techie friends get very concerned at first.
1 2 8

THE TWITTERS

Brian Phillips
@BrianRPhillips
Following

#WiFiCactus out and about in the wild @BlackHatEvents. cc:@d4rkm4tter

Crypty McCryptoFace
@mccryptoface
Following

Replying to @Grifter801 @d4rkm4tter @BlackHatEvents

Looking at this picture is making me tingly, and I'm not sure if it's because of the RF signals or my excitement.

4:28 PM - 24 Jul 2017

3 Retweets **6** Likes

Mike Szczys
@szczys
Following

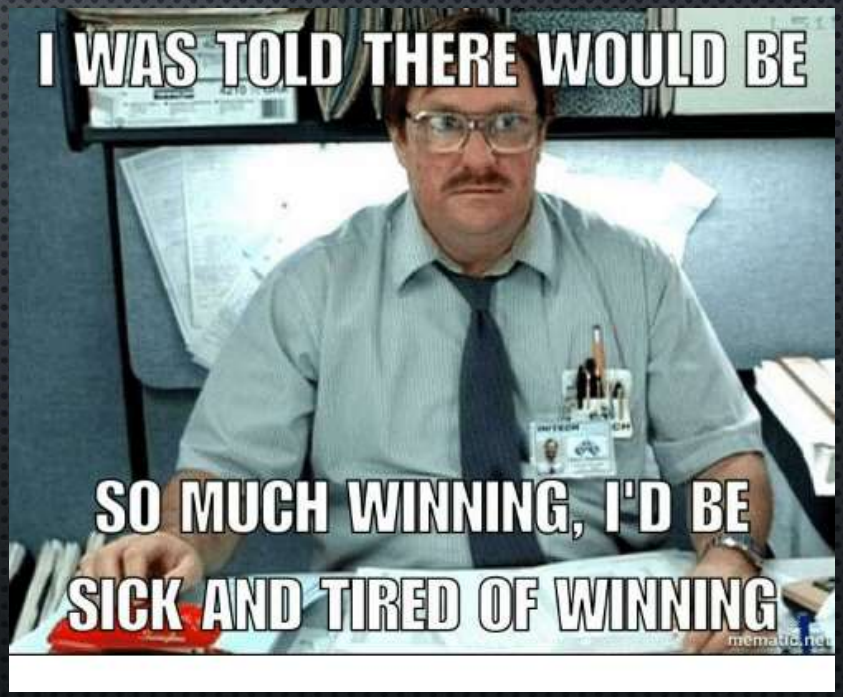
Always wear your gear to cons. #wificactus is creation of @d4rkm4tter @defcon @hackaday

6:08 PM - 29 Jul 2017

12 Retweets **47** Likes

THE WINS

- It actually worked and I pulled off multiple live demos
- didn't get detained
- Got tons of data
- The response has been amazing and humbling
- Invited to speak at DefCamp in Romania



THE FAILS

- Crashes caused the tetras to enable AP's
- It was super heavy due to lead acid battery's power density
- No car adapter
- Didn't have a voting machine attached to it

WHATS NEXT?

- More analysis
- More radios
- Maybe a Segway
- Lipos, lots of lipos
- Realtime data stats
- Data visualizations
- tactlenecks?

THANK YOU!!!!

- CONTACT INFOS:

#WIFICACTUS

PALSHACK.ORG

@D4RKM4TTER

GITHUB.COM/DARKMATTER0