Are Beacons Evil?

Keith Chew and Bill Stearns

Active Countermeasures

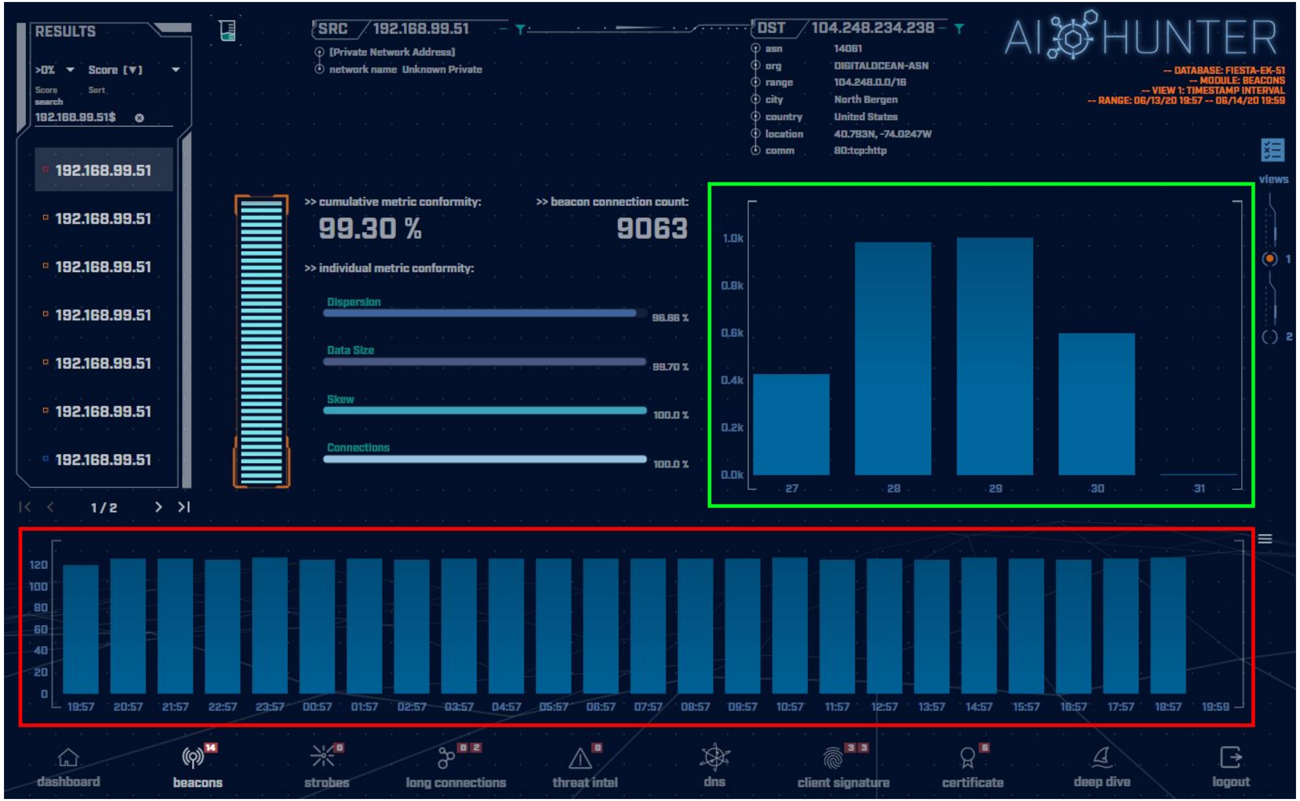
Welcome!

- Threat Hunter Community Discord
  - https://discord.gg/kEUVSNmx
  - These slides: #acm-webcast-content
  - Discussion: #live-webcast-chat
- Your speakers
  - Keith Chew
  - Bill Stearns
- Your subwoofer
  - Lexi

Threat types to consider

- Beacon
  - Multiple connections, regular intervals
  - (Strobes are high-rate-of-speed beacons)
- Long connections
  - Single or few connections held open for hours
- Are all of them malicious?

What Does a Beacon Look Like?



RESULTS

>0% Score [▼]

Score Sort

search 192.168.99.51$

192.168.99.51
192.168.99.51
192.168.99.51
192.168.99.51
192.168.99.51
192.168.99.51
192.168.99.51

1 / 2

SRC 192.168.99.51
[Private Network Address]
network name Unknown Private

DST 104.248.234.238

asn	14061
org	DIGITALOCEAN-ASN
range	104.248.0.0/16
city	North Bergen
country	United States
location	40.793N, -74.0247W
comm	80:tcp:http

-- DATABASE: FIESTA-EK-51
-- MODULE: BEACONS
-- VIEW 1: TIMESTAMP INTERVAL
-- RANGE: 06/13/20 19:57 -- 06/14/20 19:59

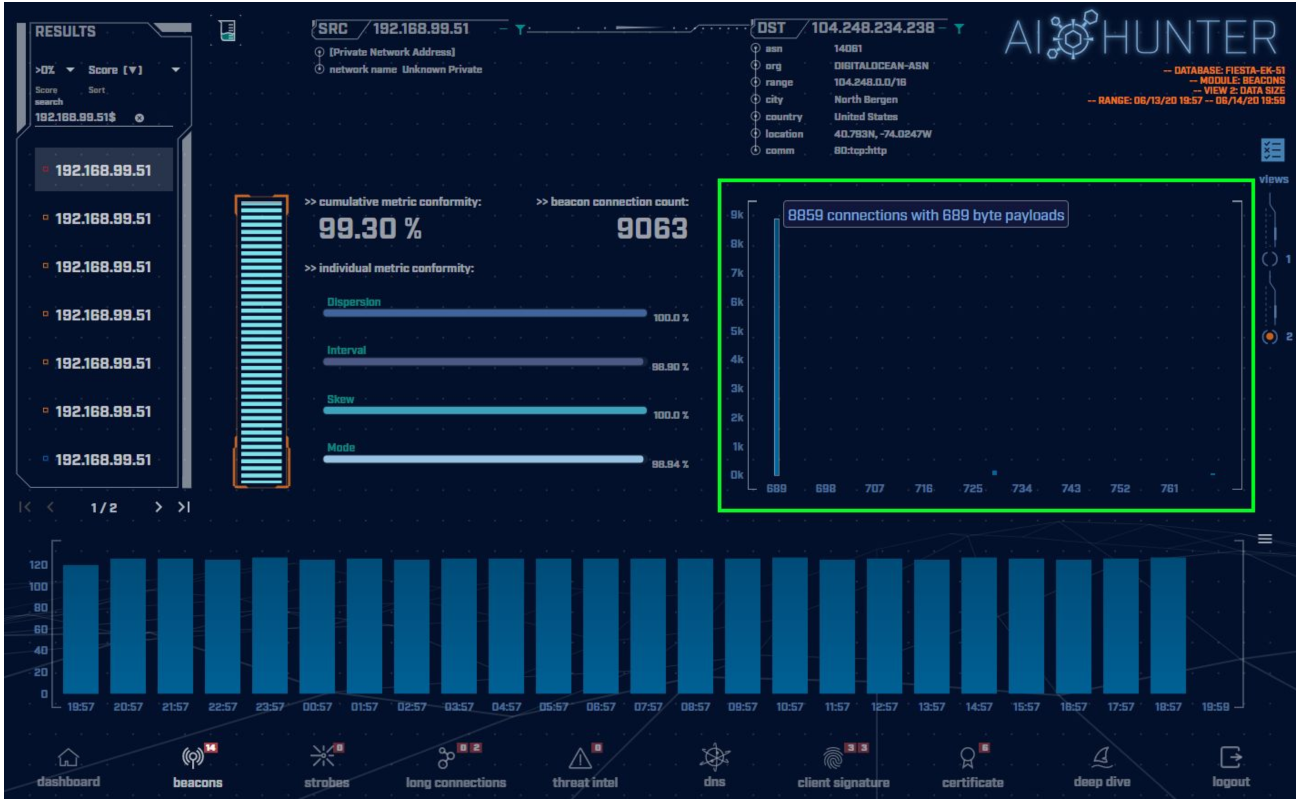
>> cumulative metric conformity: 99.30 %

>> beacon connection count: 9063

>> individual metric conformity:

Dispersion	96.66 %
Data Size	99.70 %
Skew	100.0 %
Connections	100.0 %

Data Size



RESULTS

>0% Score [▼]

Score search: 192.168.99.51$

Sort

192.168.99.51
192.168.99.51
192.168.99.51
192.168.99.51
192.168.99.51
192.168.99.51
192.168.99.51

1 / 2

SRC 192.168.99.51

[Private Network Address]

network name Unknown Private

DST 104.248.234.238

asn	14061
org	DIGITALOCEAN-ASN
range	104.248.0.0/16
city	North Bergen
country	United States
location	40.793N, -74.0247W
comm	80:tcp:http

-- DATABASE: FIESTA-EK-51
-- MODULE: BEACONS
-- VIEW 2: DATA SIZE
-- RANGE: 06/13/20 19:57 -- 06/14/20 19:59

>> cumulative metric conformity: 99.30 %

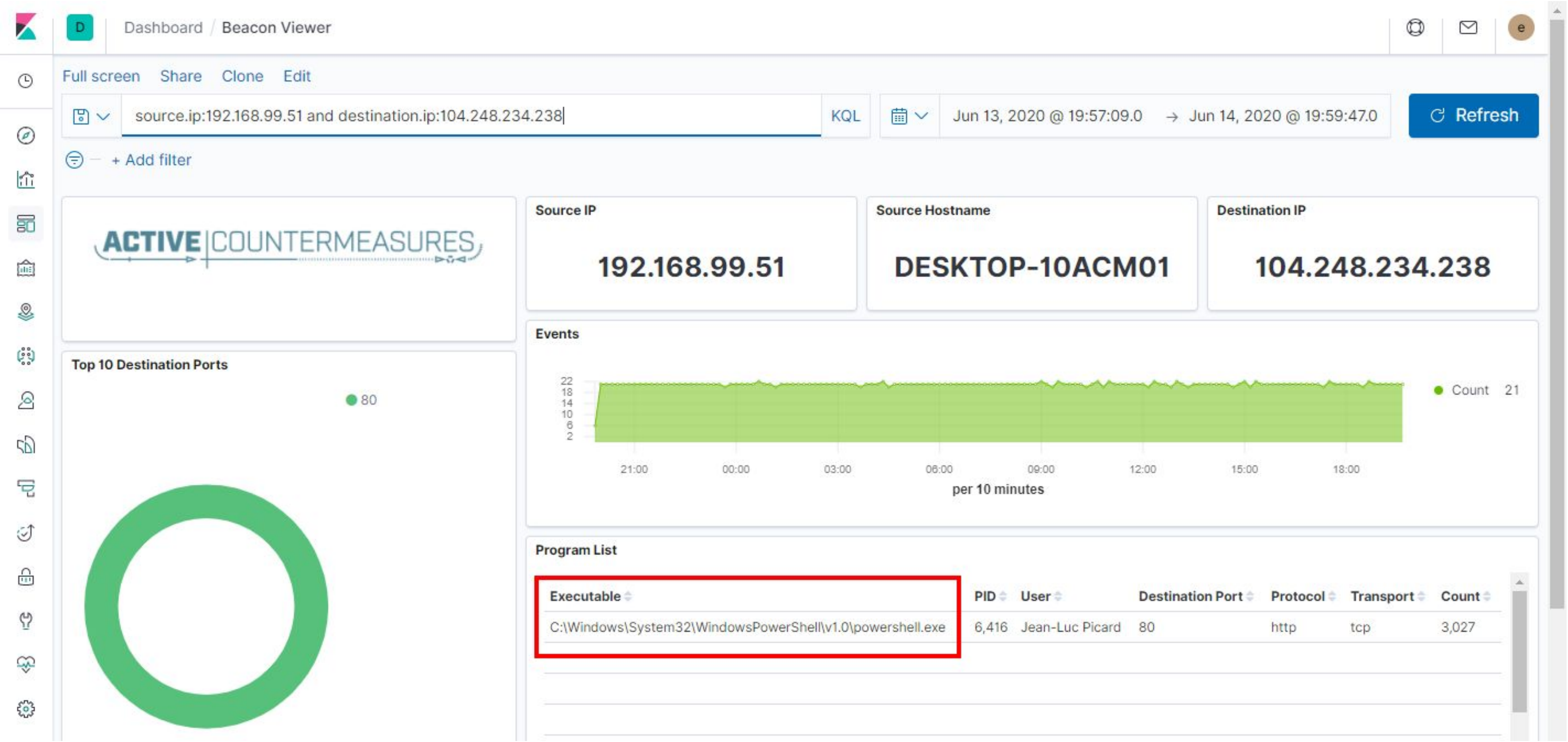
>> beacon connection count: 9063

>> individual metric conformity:

Dispersion	100.0 %
Interval	98.90 %
Skew	100.0 %
Mode	98.94 %

8859 connections with 689 byte payloads

BeaKer - view process



source.ip:192.168.99.51 and destination.ip:104.248.234.238

Jun 13, 2020 @ 19:57:09.0 → Jun 14, 2020 @ 19:59:47.0

Source IP

192.168.99.51

Source Hostname

DESKTOP-10ACM01

Destination IP

104.248.234.238

Program List

Executable	PID	User	Destination Port	Protocol	Transport	Count
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	6,416	Jean-Luc Picard	80	http	tcp	3,027

It's a Beacon, It Must Be Evil!

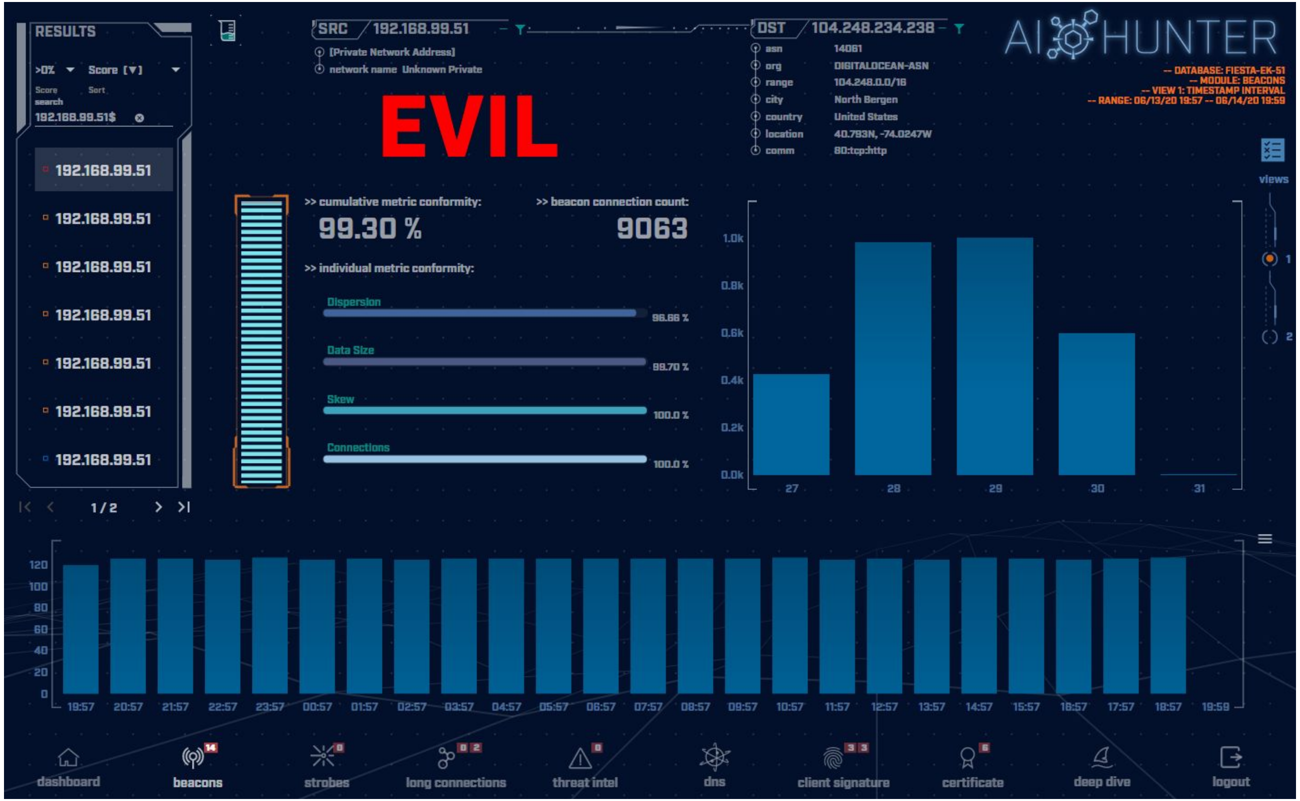
Option 1:

- Unplug everything
- Run for the hills
- Live in a cave
- Never look back

Option 2:

- Analyze and investigate

Beacon Example #1



SRC 192.168.99.51

[Private Network Address]

network name Unknown Private

EVIL

DST 104.248.234.238

asn 14061

org DIGITALOCEAN-ASN

range 104.248.0.0/16

city North Bergen

country United States

location 40.793N, -74.0247W

comm 80:tcp:http

-- DATABASE: FIESTA-EK-51
-- MODULE: BEACONS
-- VIEW 1: TIMESTAMP INTERVAL
-- RANGE: 06/13/20 19:57 -- 06/14/20 19:59

search 192.168.99.51$

>> cumulative metric conformity: 99.30 %

>> beacon connection count: 9063

>> individual metric conformity:

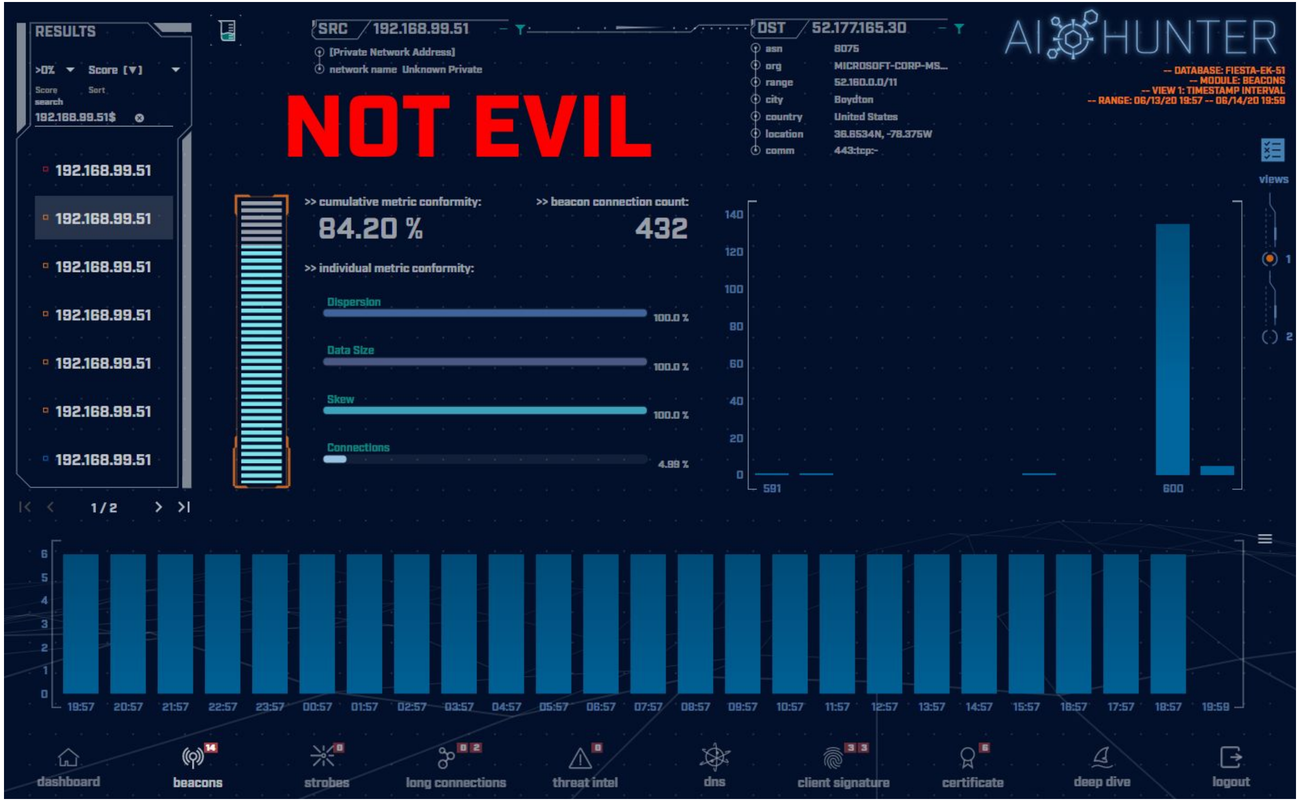
Dispersion 96.66 %

Data Size 99.70 %

Skew 100.0 %

Connections 100.0 %

Beacon Example #2



NOT EVIL

RESULTS

>0% Score

Score (▼) Sort

search 192.168.99.51$

- 192.168.99.51
- 192.168.99.51
- 192.168.99.51
- 192.168.99.51
- 192.168.99.51
- 192.168.99.51
- 192.168.99.51

1 / 2

SRC 192.168.99.51

[Private Network Address]

network name Unknown Private

DST 52.177.165.30

asn	8075
org	MICROSOFT-CORP-MS...
range	52.160.0.0/11
city	Boydton
country	United States
location	36.6534N, -78.375W
comm	443:tcp:-

-- DATABASE: FIESTA-EK-51
-- MODULE: BEACONS
-- VIEW 1: TIMESTAMP INTERVAL
-- RANGE: 06/13/20 19:57 -- 06/14/20 19:59

>> cumulative metric conformity: 84.20 %

>> beacon connection count: 432

>> individual metric conformity:

Dispersion	100.0 %
Data Size	100.0 %
Skew	100.0 %
Connections	4.99 %

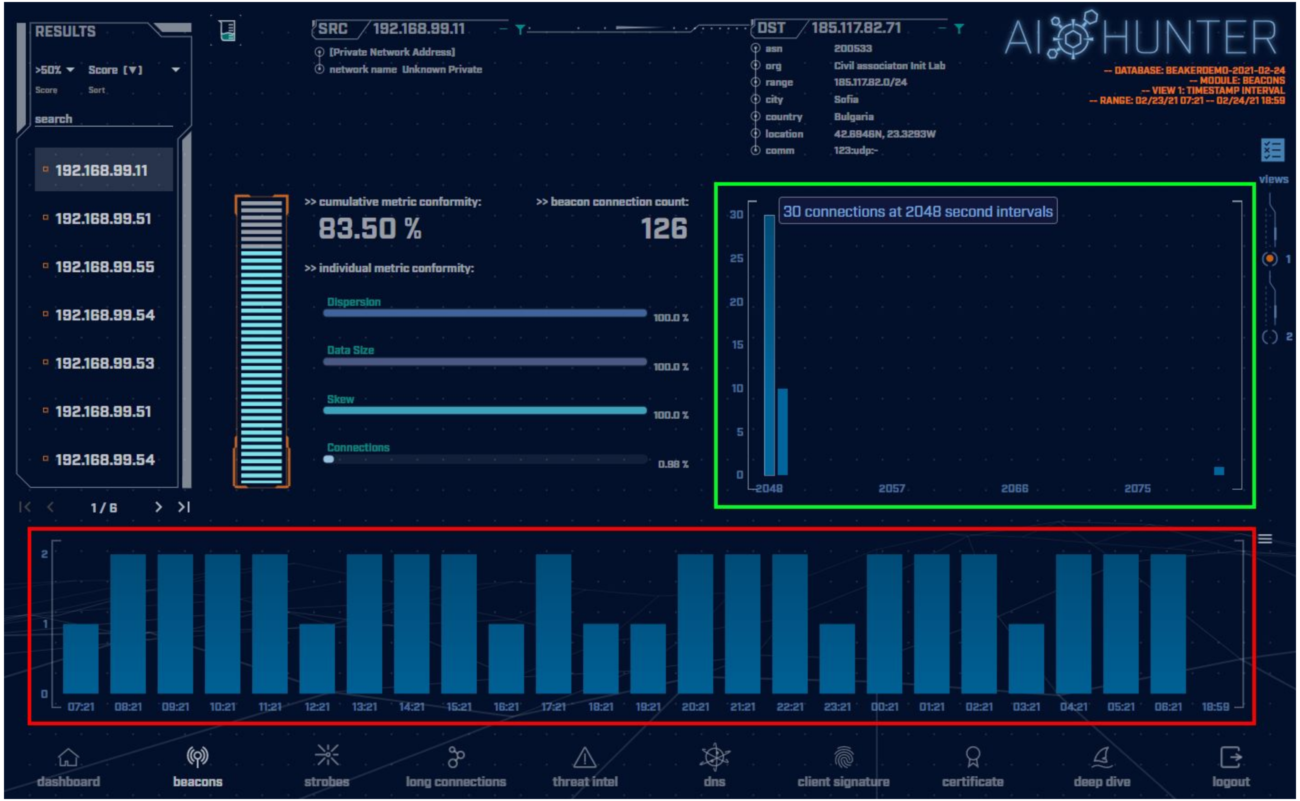
Benign traffic that look like Threats

- All too common
- Beacons and Long conns, others
  - Part of normal traffic
  - Small portion of the packet flow
  - Usually whitelistable
- Doesn't include normal user behaviour
  - Too sporadic
  - Scores low

NTP

- Your clients talking to NTP server(s)
- UDP port 123
- Benign beacon, regular timing
- Regular check ins to small group of IPs
- Whitelist/Filter
  - "*.pool.ntp.org"
  - All NTP protocol traffic
  - UDP port 123

NTP Beacon



RESULTS

>50% Score

Score [▼] Sort

search

- 192.168.99.11
- 192.168.99.51
- 192.168.99.55
- 192.168.99.54
- 192.168.99.53
- 192.168.99.51
- 192.168.99.54

1 / 6

SRC 192.168.99.11

[Private Network Address]

network name Unknown Private

DST 185.117.82.71

asn	200533
org	Civil associaton Init Lab
range	185.117.82.0/24
city	Sofia
country	Bulgaria
location	42.6946N, 23.3293W
comm	123:udp:-

-- DATABASE: BEAKERDEMO-2021-02-24
-- MODULE: BEACONS
-- VIEW 1: TIMESTAMP INTERVAL
-- RANGE: 02/23/21 07:21 -- 02/24/21 18:59

>> cumulative metric conformity: 83.50 %

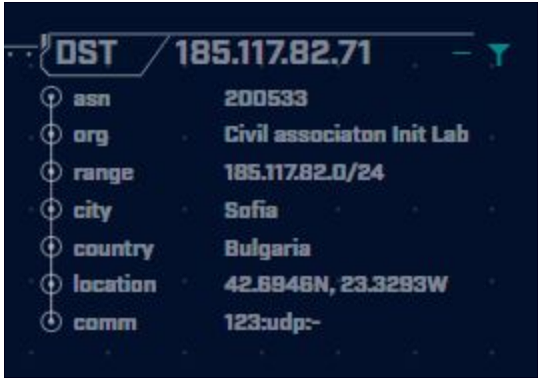
>> beacon connection count: 126

>> individual metric conformity:

Dispersion	100.0 %
Data Size	100.0 %
Skew	100.0 %
Connections	0.98 %

30 connections at 2048 second intervals

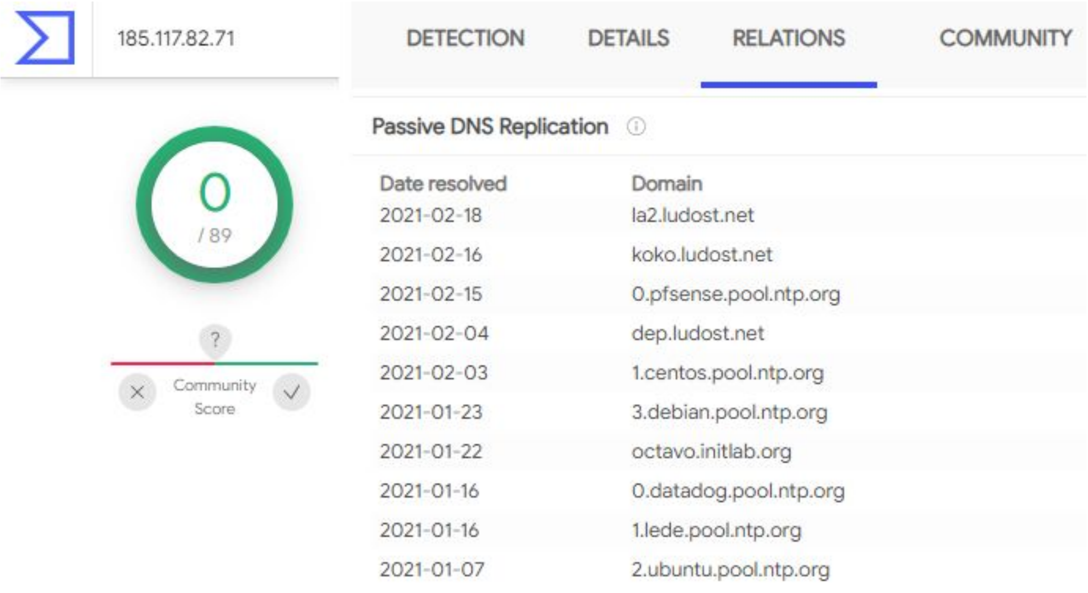
NTP Beacon Destination



DST 185.117.82.71

asn	200533
org	Civil associaton Init Lab
range	185.117.82.0/24
city	Sofia
country	Bulgaria
location	42.6946N, 23.3293W
comm	123:udp:-

NTP Beacon Investigation



185.117.82.71

Passive DNS Replication

Date resolved	Domain
2021-02-18	la2.ludost.net
2021-02-16	koko.ludost.net
2021-02-15	0.pfsense.pool.ntp.org
2021-02-04	dep.ludost.net
2021-02-03	1.centos.pool.ntp.org
2021-01-23	3.debian.pool.ntp.org
2021-01-22	octavo.initlab.org
2021-01-16	0.datadog.pool.ntp.org
2021-01-16	1.lede.pool.ntp.org
2021-01-07	2.ubuntu.pool.ntp.org

- virustotal.com

VPN traffic

- Steady traffic between VPN endpoints
- Could appear as Beacon, Strobe, or Long Conn
- Ports
  - 1194/UDP (openvpn)
  - Protocol 50 and 500/UDP (ipsec)
  - 22/TCP (ssh)
  - 4501/UDP, 443/TCP (Globalprotect)

VPN

- Whitelist/Filter
  - IP Pairs of endpoints
  - By Protocol used
  - By specific ports and protocols
- Caution
  - VPNs could hide malicious traffic
  - True of any tunneling approach

OS/App patching

- Beacons, Client signature
- Commonly 443/TCP
- Whitelist
  - By FQDN/domain
  - By ASN
  - By IP

BGP traffic between routers

- Visible on inter-router segments
- 179/TCP
- Whitelist/Filter
  - By router IP pairs
  - By BGP protocol
  - By port 179/TCP

SQL server replication

- Traffic between primary and secondary
- Long connection
- 3306/TCP, 5432/TCP, 1434/TCP
- Whitelist/Filter
  - By IP pairs
  - By protocol if recognized
  - By port number

Network monitoring tools

- Regular probes to existing servers
- Probing legitimate service ports
- Whitelist
  - Source IP: monitoring server(s)
    - Make sure systems are locked down
  - By IP pairs (monitor -> monitored server)

Remote access apps

- Evil or not? It depends
- Expected/allowed
- Business hours only?
- Amount of data transferred
- Usage restrictions

MS: 443/TCP

- Long connections
  - Dnscat2-ja3, long conns,
- Whitelist
  - Top level domain
  - ASN 8075
    - Mix of good and bad
  - Subnet

Chat/VOIP apps

- Beacons or Long connections
- Slack, Skype, Meet, Hangout, Teams, IRC
  - File transfer!
- Whitelist
  - By FQDN or domain
  - By ASN
  - By destination IP (if anyone can connect)
  - By IP pair (if only a few systems can connect)

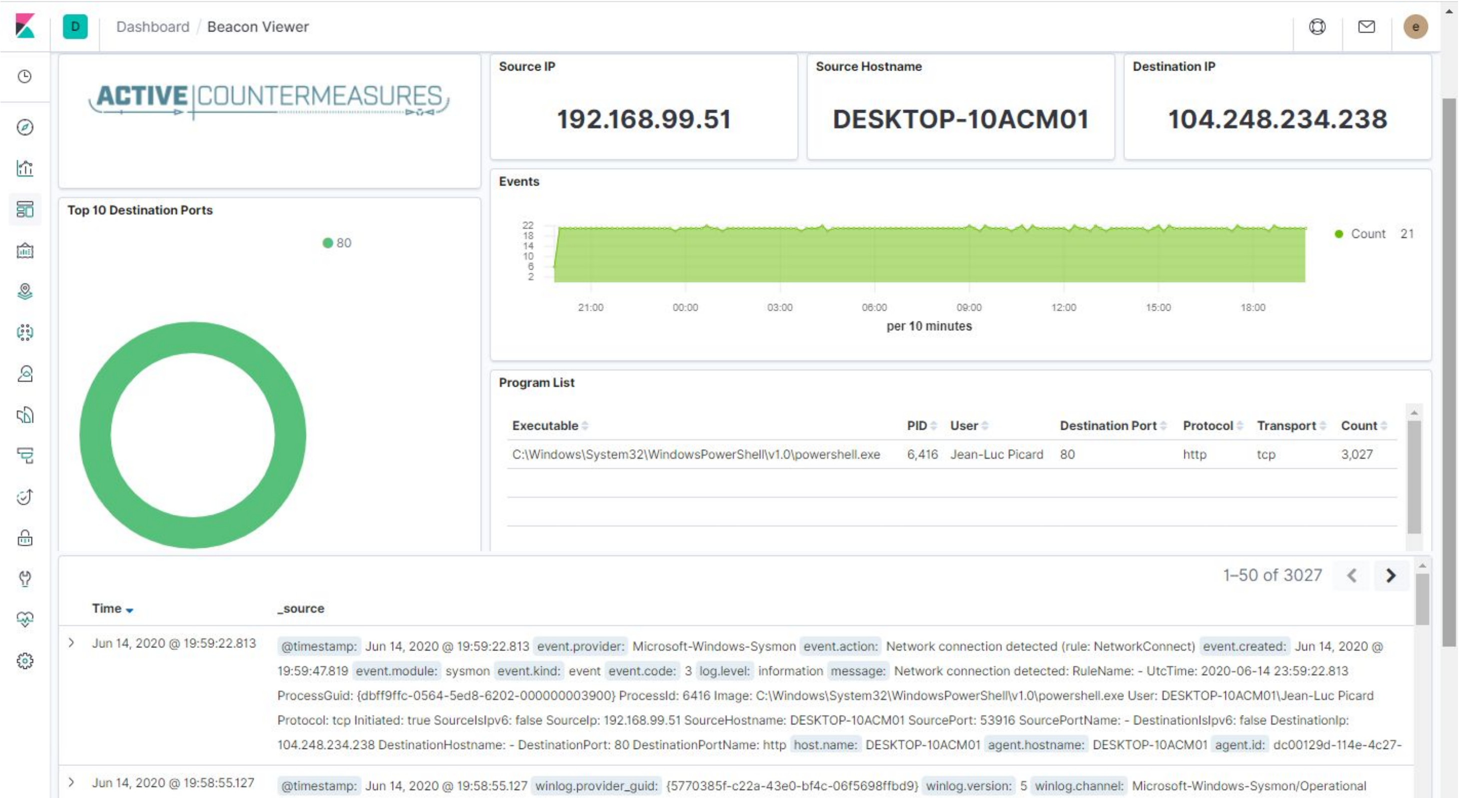
Advertising traffic

- Example domains:
  - adnxs.com
  - casalemedia.com
  - doubleclick.net
  - googleadservices.com
  - taboola.com
- Handling
  - Ad blocking plugin
  - firewalling

What if I don't know?

- Traffic not clearly benign or malicious
- Check
  - Port and detected protocol
  - ASN/Hostname
  - Source system: what does the system do?
  - Allowed by policy?
    - Source system OS/apps: allowed to connect?
  - Application generating it on your client
    - Check processes on system
    - BeaKer :-)

BeaKer



Source IP: 192.168.99.51

Source Hostname: DESKTOP-10ACM01

Destination IP: 104.248.234.238

Program List

Executable	PID	User	Destination Port	Protocol	Transport	Count
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	6,416	Jean-Luc Picard	80	http	tcp	3,027

1-50 of 3027

Time	_source
Jun 14, 2020 @ 19:59:22.813	@timestamp: Jun 14, 2020 @ 19:59:22.813 event.provider: Microsoft-Windows-Sysmon event.action: Network connection detected (rule: NetworkConnect) event.created: Jun 14, 2020 @ 19:59:47.819 event.module: sysmon event.kind: event event.code: 3 log.level: information message: Network connection detected: RuleName: - UtcTime: 2020-06-14 23:59:22.813 ProcessGuid: {dbff9ffc-0564-5ed8-6202-000000003900} ProcessId: 6416 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe User: DESKTOP-10ACM01\Jean-Luc Picard Protocol: tcp Initiated: true SourceIsIpv6: false SourceIp: 192.168.99.51 SourceHostname: DESKTOP-10ACM01 SourcePort: 53916 SourcePortName: - DestinationIsIpv6: false DestinationIp: 104.248.234.238 DestinationHostname: - DestinationPort: 80 DestinationPortName: http host.name: DESKTOP-10ACM01 agent.hostname: DESKTOP-10ACM01 agent.id: dc00129d-114e-4c27-
Jun 14, 2020 @ 19:58:55.127	@timestamp: Jun 14, 2020 @ 19:58:55.127 winlog.provider_guid: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} winlog.version: 5 winlog.channel: Microsoft-Windows-Sysmon/Operational

Whitelisting support

- RITA
  - Not built in, but can via grep
- Firewall
  - By src/dest IP, subnet, port
  - Sometimes logged-in user or hostname
- AC-Hunter
  - By src/dest IP, ASN, subnet
  - By IP pair
  - And one more thing.... :-)

References

- Blogs
  - https://www.activecountermeasures.com/threat-hunting-false-positives/
    - RITA whitelisting section
  - https://www.activecountermeasures.com/suspicious-traffic-found-what-are-the-next-steps/
    - Rich set of investigation ideas
  - https://www.activecountermeasures.com/malware-of-the-day-attack-vectors-teamviewer/

Software shown in this webcast

- AC-Hunter
  - https://www.activecountermeasures.com/ac-hunter-features/
- BeaKer
  - https://github.com/activecm/BeaKer
- RITA
  - https://github.com/activecm/rita/

Thanks, and Questions?

- Keith and Bill for presenting
- Hannah, Kris, and Ryan for answering questions
- Shelby for setting up the presentation
- Questions?