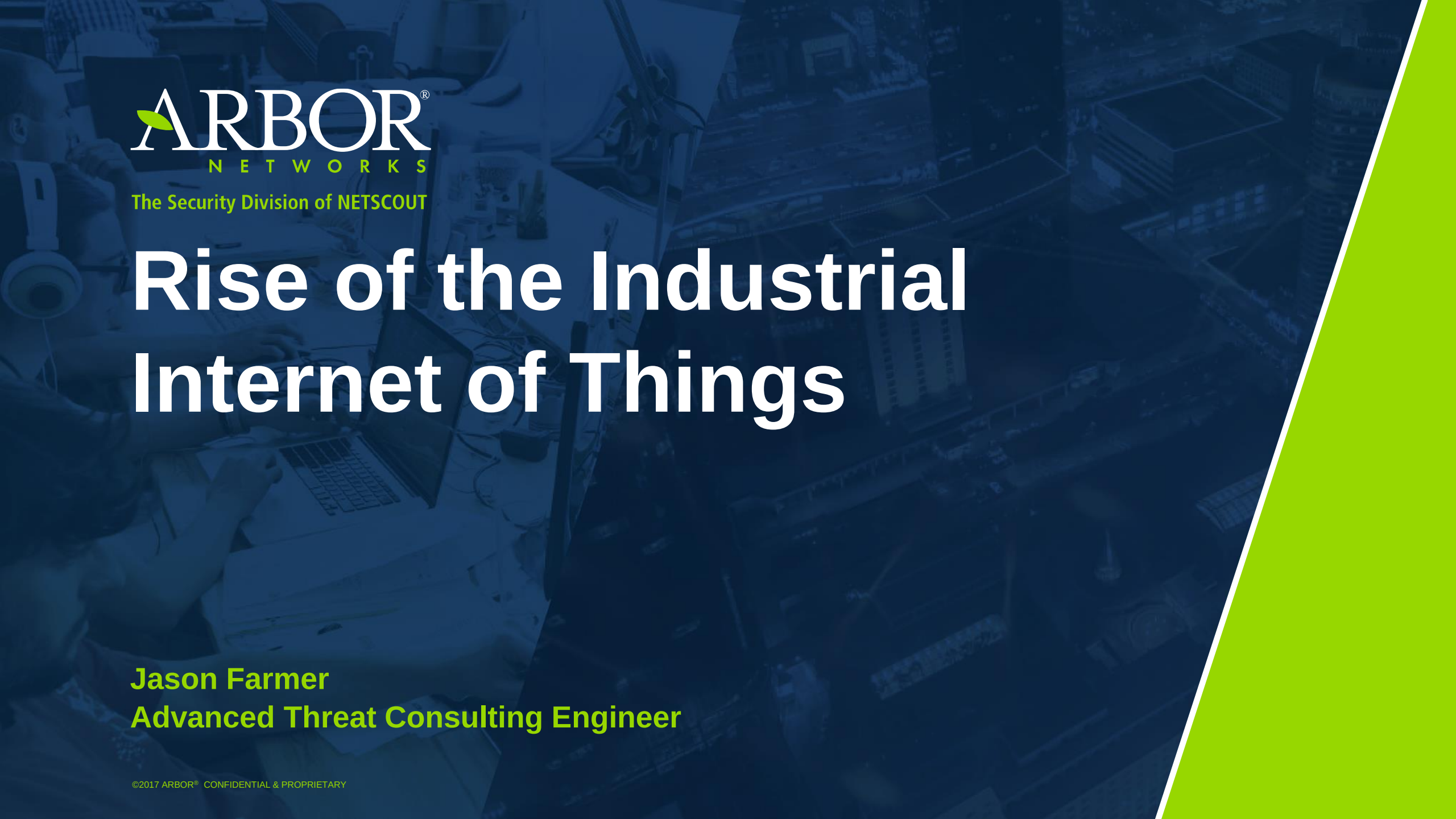


ARBOR NETWORKS
The Security Division of NETSCOUT

Rise of the Industrial Internet of Things

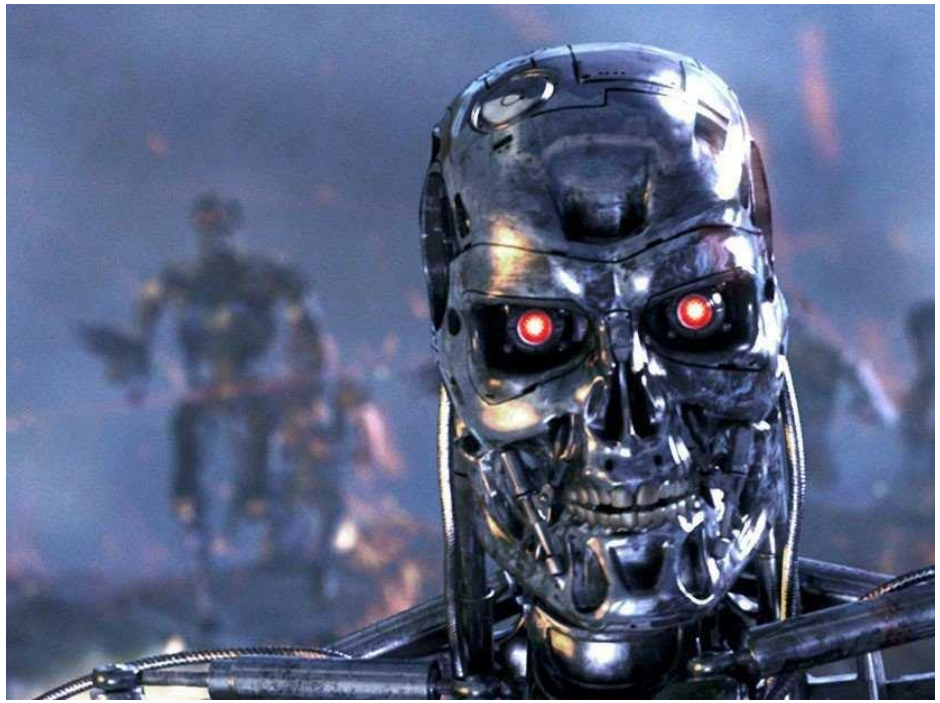
Jason Farmer
Advanced Threat Consulting Engineer

What is the Industrial Internet of Things

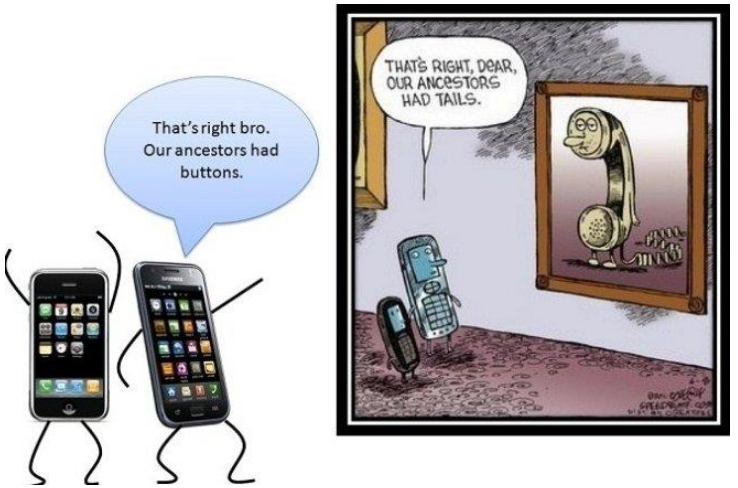
The Industrial Internet of Things (IIoT), also known as the Industrial Internet, brings together brilliant machines, advanced analytics, and people at work. It's the network of a multitude of devices connected by communications technologies that results in systems that can monitor, collect, exchange, analyze, and deliver valuable new insights like never before. These insights can then help drive smarter, faster business decisions for industrial companies.

What Does the Really Mean?

- Thousands, if not millions, of new devices (IoT)
- Bi-directional communications with production systems
- Big Data
- Machine learning



IoT is Like BYOD on Steroids



- An order of magnitude more devices
- Hide in plain site
- May not be vetted by your IT department
- Security standards don't exist
- Patching procedures are spotty if they exist at all
- Mobile phones are the largest category of connected devices at the moment, but will be exceeded by IoT sensors and devices in 2018

I will Air Gap These IoT devices

Can you really air gap these systems?

Even if you can consider the following:

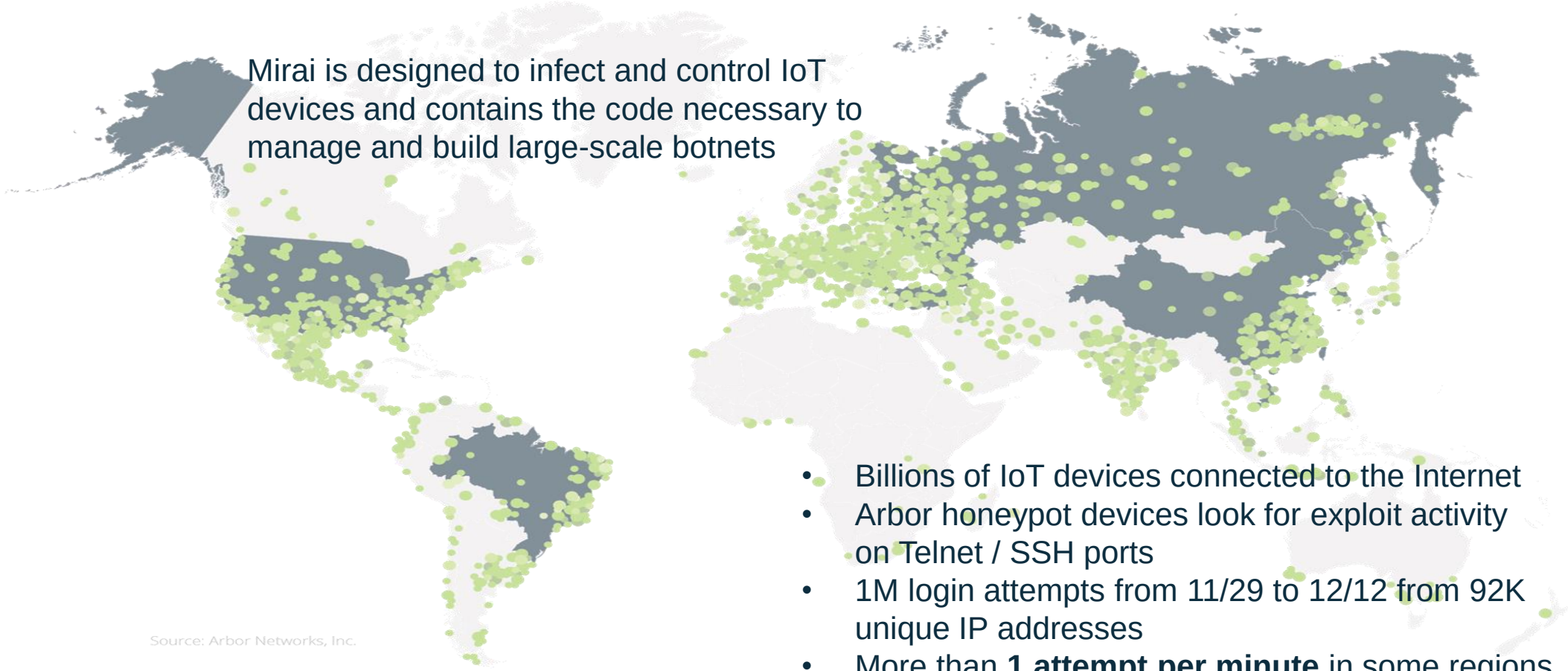
- Stuxnet
- Agent.btz
- BitWhisper
- Brutal Kangaroo

Securing IoT Devices

- You should know that smart products currently exist in your enterprise.
- Here are the most important steps to take to manage and secure these devices.
  - Identify which devices have communication capabilities. If a device connects to your network and sends alerts, communicates with its manufacturer for warranty updates or provides any other indication that it is using its network connection to reach outside the enterprise, add it to your list of enabled systems.
  - Connect devices to your network only if there is a demonstrable benefit. If a device can function properly without a network connection or if its connection only provides marginal utility, disconnect it and test its functionality. Before reconnecting, ask the manufacturer how the product is intended to communicate and what measures have been taken to secure it.
  - Create separate networks specifically for smart device connections.
  - Disable Universal Plug and Play (UPnP). Do not allow automatic discovery and connection for networked devices. Make certain that any devices that request network access are reviewed for security and connected to the proper network segment.
  - Update firmware where possible. Contact manufacturers for updates to their firmware and ask about procedures they have taken to add security measures to the systems you use.

IOT Threats? I Give You Mirai's Machine

Mirai is designed to infect and control IoT devices and contains the code necessary to manage and build large-scale botnets



- Billions of IoT devices connected to the Internet
- Arbor honeypot devices look for exploit activity on Telnet / SSH ports
- 1M login attempts from 11/29 to 12/12 from 92K unique IP addresses
- More than **1 attempt per minute** in some regions

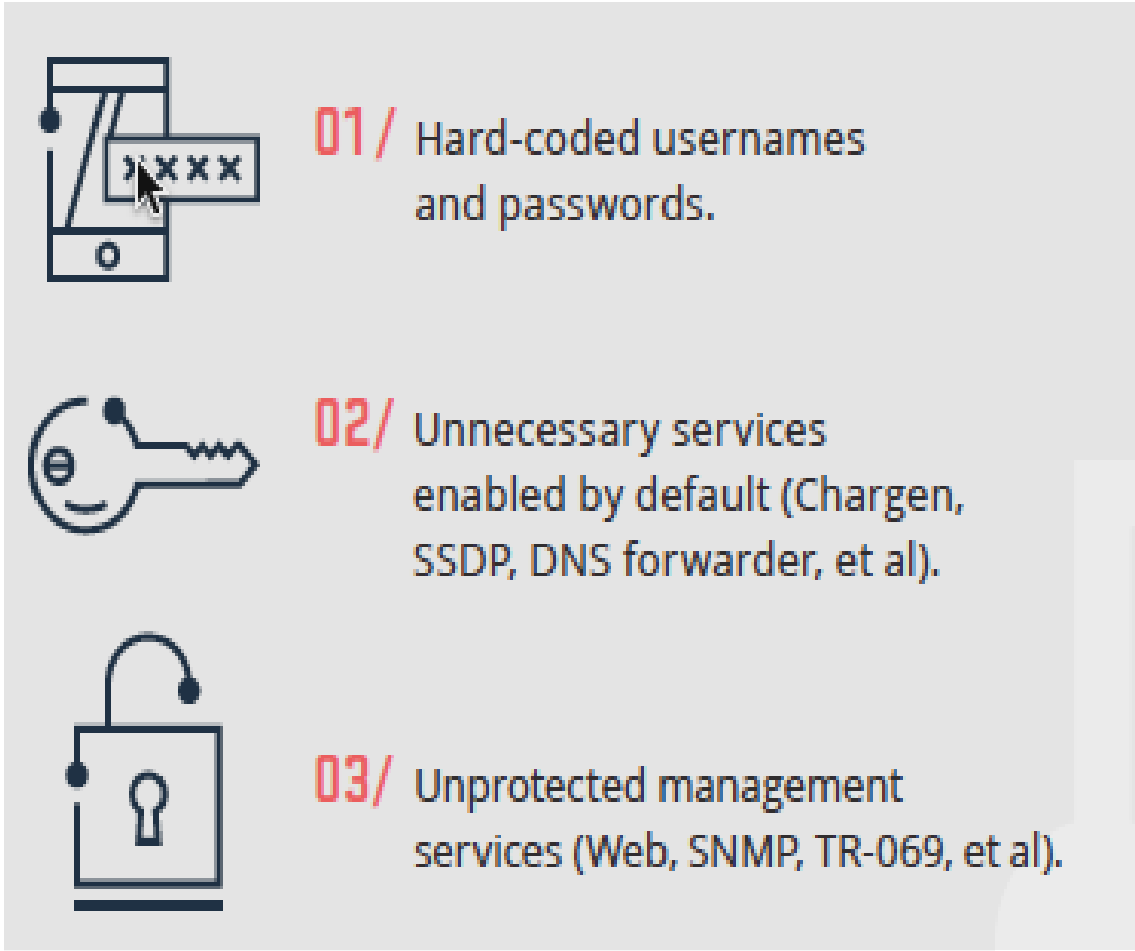
Driving Factors, IoT

The Problem

- Devices are designed to be easy to deploy and use, often resulting in limited security capabilities
- Software is very rarely upgraded. Some manufacturers don't provide updates, or the ability to install updates

The Result

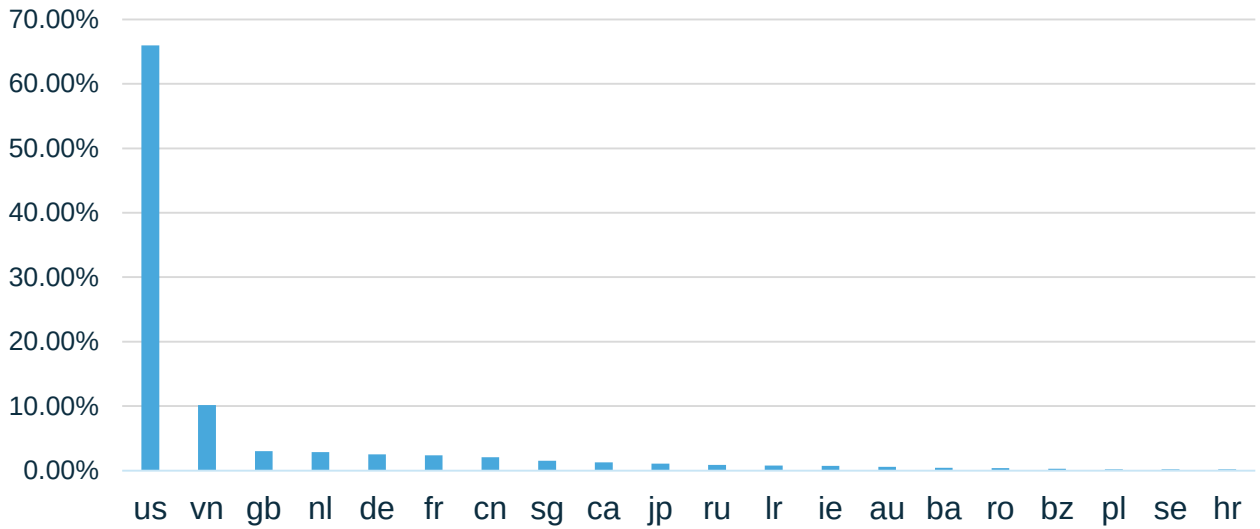
- First high-profile attack using IoT devices Christmas 2013, using CPE and webcams
- In 2016 Botnet owners started to recruit IoT devices en mass
- Attacks of 540Gbps against the Olympics, 620Gbps against Krebs, Dyn etc..



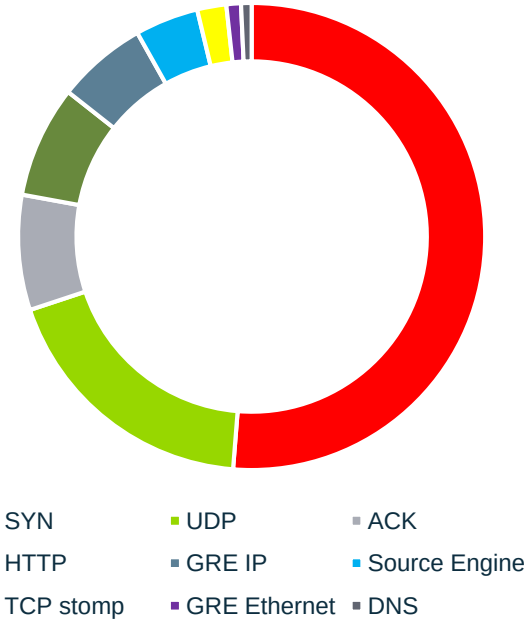
How Arbor Helps with IoT Awareness

- Not one but two networks of honeypots looking at IoT threats!
  - Can see new behaviors, sources, reverse binaries etc..
- Infiltration of multiple IoT Botnets for DDoS monitoring
  - Monitored 11412 attacks over 3 month period.

Attack Target Locations



Mirai Attack Types



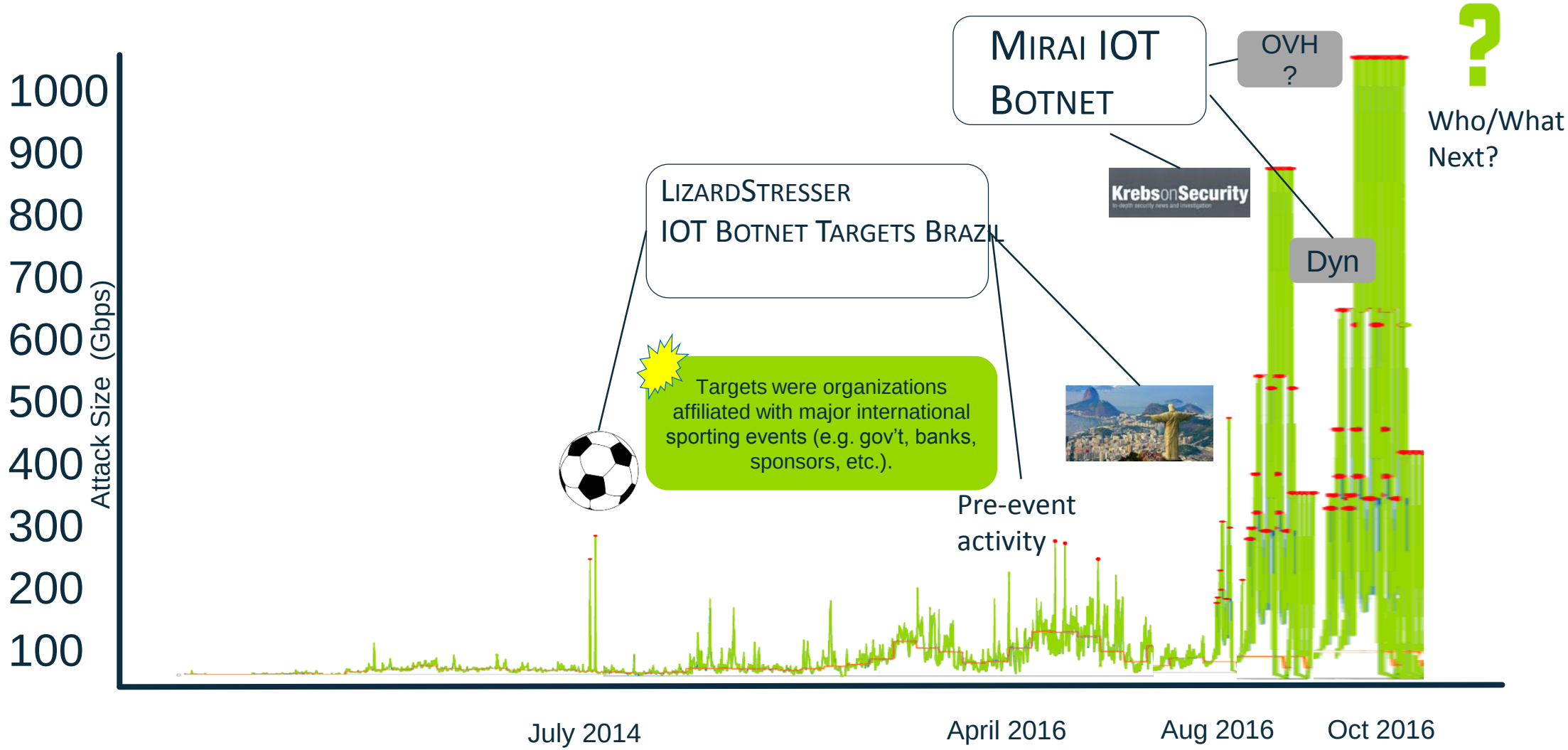
The History of IoT Botnets

Iot botnets are actually nothing new:

- The first bot was created back in 1993 when Robey Pointer created an Internet Relay Chat (IRC) bot called “eggbot” which was used to manage and protect IRC channels against takeover attempts. Multiple instances of the bot could work together in “botnets” to defend against DDoS attacks.
- In 2003, the first (unintentional) DDoS attack against the University of Wisconsin using IoT devices happened due to a hardcoded NTP address in 700.000 Netgear DSL/cable modems. Even after a new software was released, the attack continued for years until the last device was chucked in the bin.
- In 2008, the first recorded DDoS IoT botnet attack was done using a botnet of Linux based CPE broadband routers.
- In 2012, an unknown researcher published a report called the “Internet census of 2012”. The data used in the report was gathered by hacking into an estimated 420,000 CPE devices around the world using default credentials[1]

1) https://en.wikipedia.org/wiki/Carna_botnet

IoT Botnets Are Not New and On The Rise



Who Wants to Inform and Protect You

IoT Security Foundation

Our Mission

Our mission is to help secure the Internet of Things, in order to aid its adoption and maximise its benefits. To do this we will promote knowledge and clear best practice in appropriate security to those who specify, make and use IoT products and systems.

Make it safe to connect

The Next Magic Quadrant?

MOCANA

ARGUS
CYBER SECURITY

THETARAY

PWNIE EXPRESS

Indegy

PFP
CYBERSECURITY

Rubicon

Bastille
SECURITY FOR THE INTERNET OF RADIOS

CyberX

SECURE RF

DEVICE AUTHORITY
IoT Security Simplified

ZITOVAULT

NEXDEFENSE

BAYSHORE
INDUSTRIAL-STRENGTH CYBERSECURITY

Karamba Security

ZingBox

Trillium

ARBOR NETWORKS

Q&A / Thank You

For more info, please contact:

Jason Farmer
Advanced Threat Sales Engineer
jfarmer@arbor.net

ARBOR NETWORKS
The Security Division of NETSCOUT