# The Security Risks of Orphaned Network Traffic

BitSight Security Labs

www.bitsighttech.com

# Agenda

1. Methodology
2. Orphan traffic observations
3. Metrics - Geographies, sectors
4. Q&A

# Research methodology

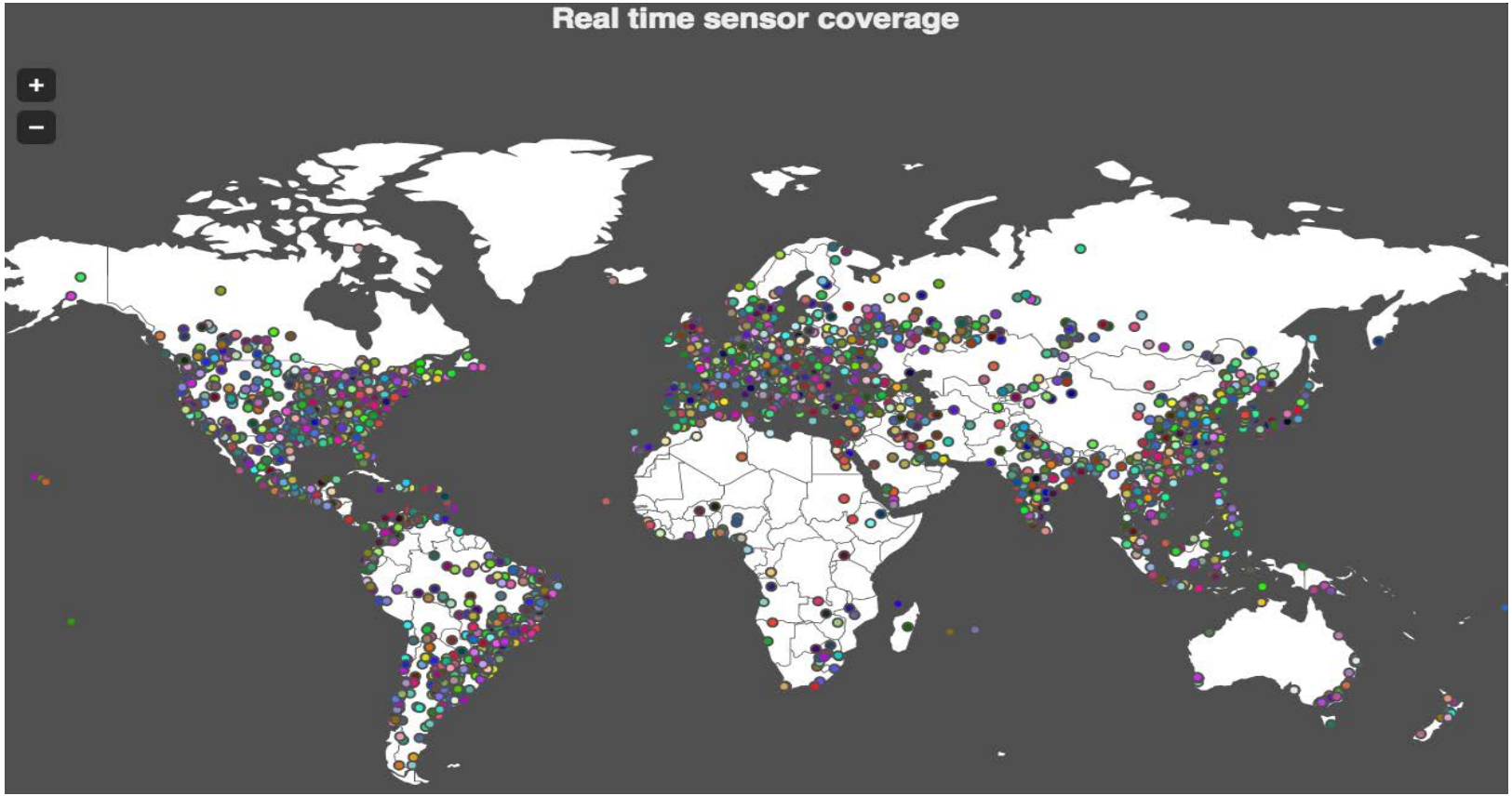
# On the research process

- Continuous monitorization of world wide network traffic for the purpose of identifying potential malicious communications
- Covering multiple geographies, industries, sectors
- Using automated methods, looking for patterns, frequency ..

- Special focus on:
  - Web traffic ( HTTP/S )
  - DNS traffic
  - EMail traffic ( SMTP )

Taking over malicious **NXDOMAINS** for the purpose of measuring and tracking worldwide infections and malware campaigns

# Traffic observations worldwide



# A sea of data...

42,120 Events per second

3,639,168,000 .. daily

**1,328,296,320,000** … yearly

# A sea of data...

# The wrong type of fish in the net

1) Non malicious traffic ( by intent )

2) Found as a byproduct of the research around potential malicious traffic

3) Not normally red flagged by security focused technology ( after all, “it’s all legit” )

Main categories observed:

- Miss configurations
- Policy control failures
- Abandoned applications & software
- Device/appliance firmware

# Orphan traffic observations

The wrong type of fish in the net

# gTLDs, expired/unused domains and DNS suffix issues

# The wrong type of fish in the net

- The new gTLDs chaos
  - *.global
  - *.work
  - *.home
  - *.network
  - ….

*myserver.home*

*importantservice.work*

*gateway.network*

***wpad.work***

- Expired or unused domains
  - “mynetwork.com” , “myservice.net”

# The wrong type of fish in the net

- The new gTLDs chaos
  - *.global
  - *.work
  - *.home
  - *.network
  - ….

*myserver.home* 

*importantservice.work* 

*gateway.network* 

***wpad.work*** 

- Expired or unused domains
  - “mynetwork.com” , “myservice.net”

# The Proxy config nightmare

## Exploiting wpad/proxy.pac proxy auto-discovery and configuration

# Proxy config

- *“The Web Proxy Autodiscovery Protocol (**WPAD**) is a method used by clients to locate the URL of a configuration file using DHCP and/or **DNS discovery** methods. Once detection and **download of the configuration file** is complete, it can be executed to **determine the proxy** for a specified URL.” -* *https://en.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol*

# Proxy config in a nutshell

1. Web clients (such as browsers) look for *wpad.<domain>* for fetching proxy configuration
2. Browsers can also be configured to retrieve specific proxy configurations from pre configured URIs ( e.g. *hxxp://proxycfg.oldinternaldomain.com/proxy.pac*)

3. If the hostname exists, or there's a pre configured URI, the web client will fetch the configuration file

4. Proxy configuration file dictates which proxy address the client should use, and on which circumstances

```
return "PROXY 1.2.3.4:8080"
```

# Proxy config hijack

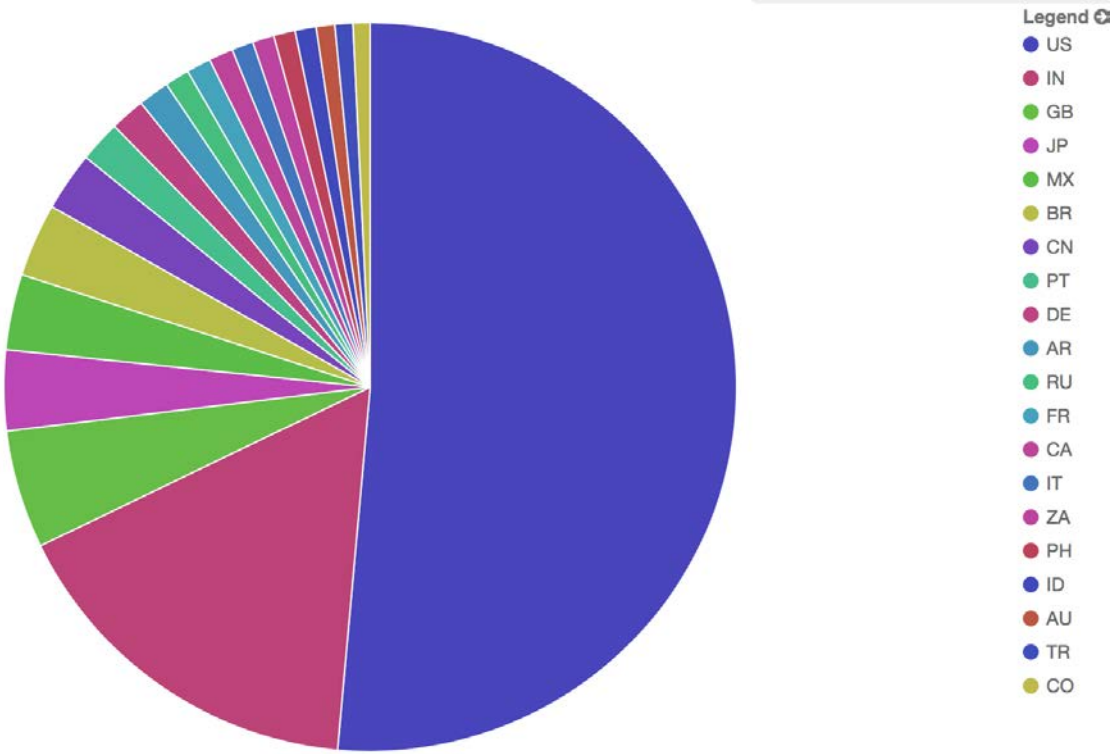
- Web traffic hijack made easy
  - Internal old domains that eventually drop
  - gTLD domains that used to be “safe”
- Impact:
  - Relatively simple to exploit
  - In essence MitM over the web traffic
    - Access to all traffic
    - Traffic manipulation ( e.g. inject/replace malicious content )
    - Authorization credentials hijack

# Proxy config hijack - a real example

The recent *Acme* big company real case (July 2016)

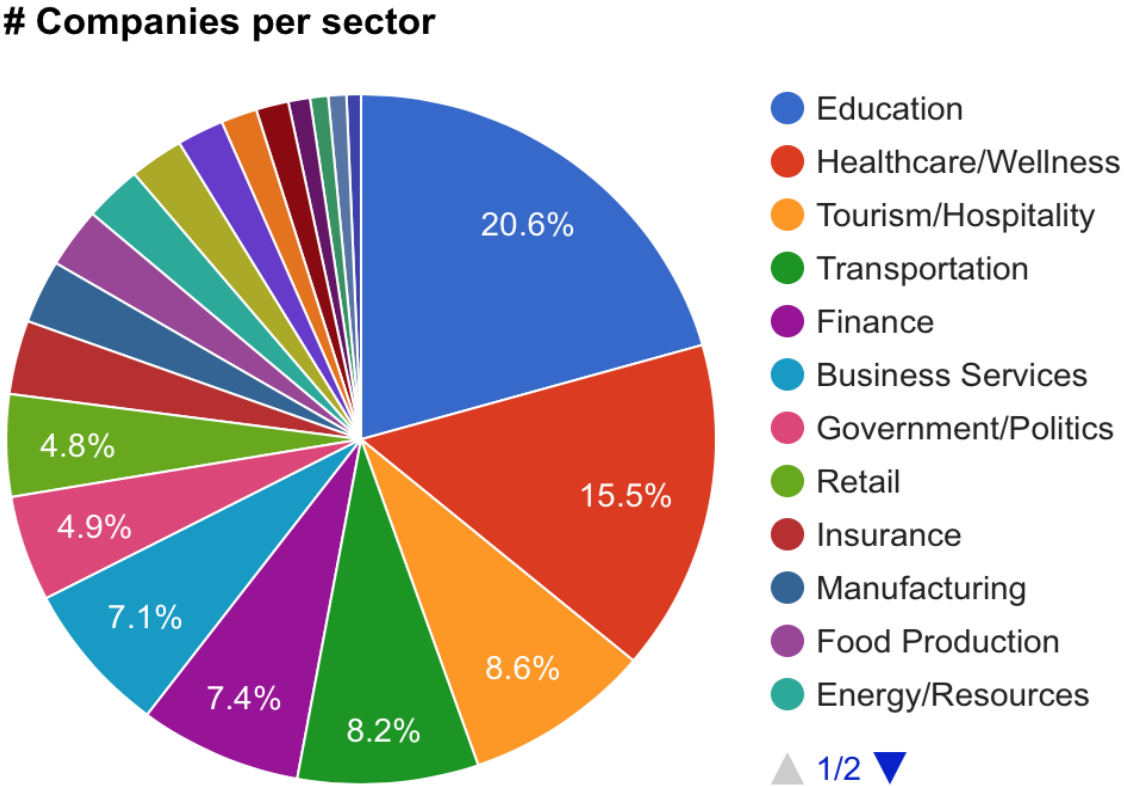
- *Acme* reached out to us on anomalous traffic observed directed to our servers
- Initial research determined it to be **proxy configuration requests**
- Further investigation revealed that several laptops recently acquired from a **well known manufacturer** were the origin of the traffic
- These laptops came with a **default DNS configuration** pointing to a non-existent domain
- For a brief period of time, this US based company had all their

# Proxy config problem - How wide spread?




**64,872,110** Proxy config requests processed

# Proxy config problem - How wide spread?




**64,872,110** Proxy config requests processed

Abandoned software/apps

**Examples and associated risks**

# Abandonware

“***Abandonware*** *is a product, typically software, ignored by its owner and manufacturer, and for which no product support is available*” - Wikipedia

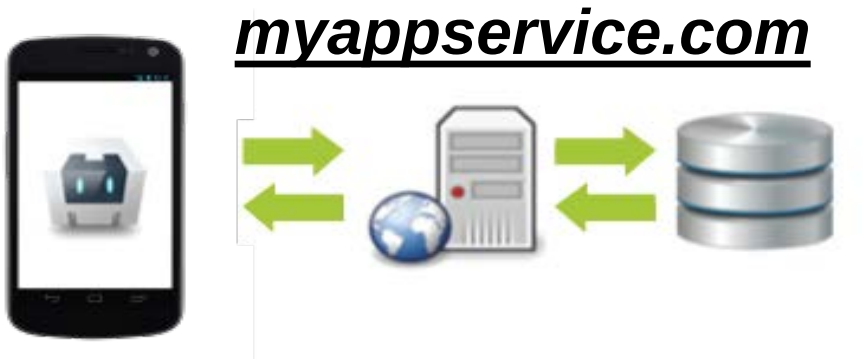
# Abandonware - Mobile apps

- The mobile app example
  - Creative ideas -> successful “apps” , anyone can do it
  - Easy to get, easy to install, often easy to forget it’s there



# Abandonware - Mobile apps

- Often, apps will use servers and contact custom domain names for arbitrary tasks:
  - Configuration changes
  - App updates
  - Publishing information
  - ...

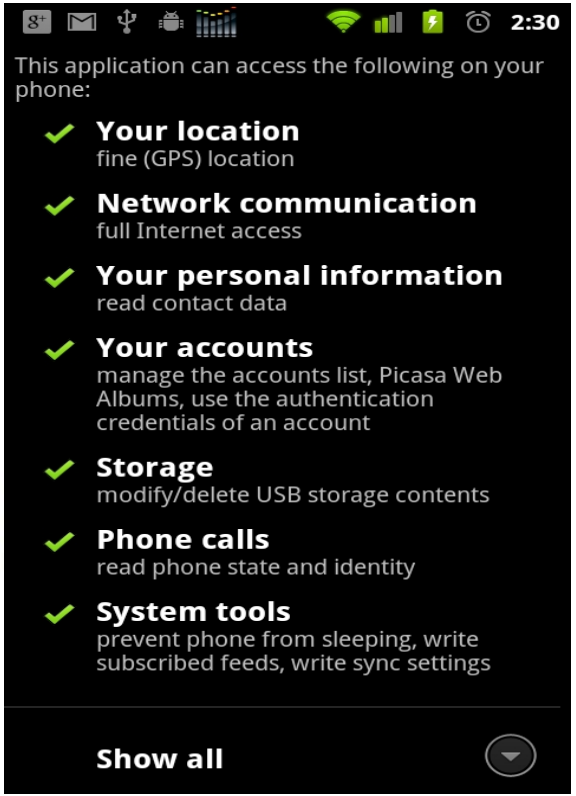


# Abandonware - Mobile apps

- Often, apps will use servers and contact custom domain names for arbitrary tasks:
  - Configuration changes
  - App updates
  - Publishing information
  - ...

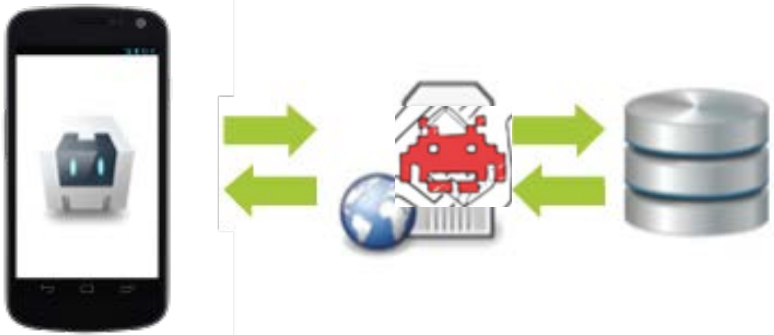
# Abandonware - Mobile apps

- Often, apps will use servers and contact custom domain names for arbitrary tasks:
  - Configuration changes
  - App updates
  - Publishing information
  - ...



# Abandonware - Mobile apps

- The result: Information in the wild
  - IMEIs, Mobile phone numbers
  - Personal information
  - Contact data
  - Text messages
  - Photos
  - Call logs
  - GPS data (geo localization)
  - Application specific data



# Abandonware - Not just mobile apps

**The Android firmware “incident”** - Yet another strange fish on the net

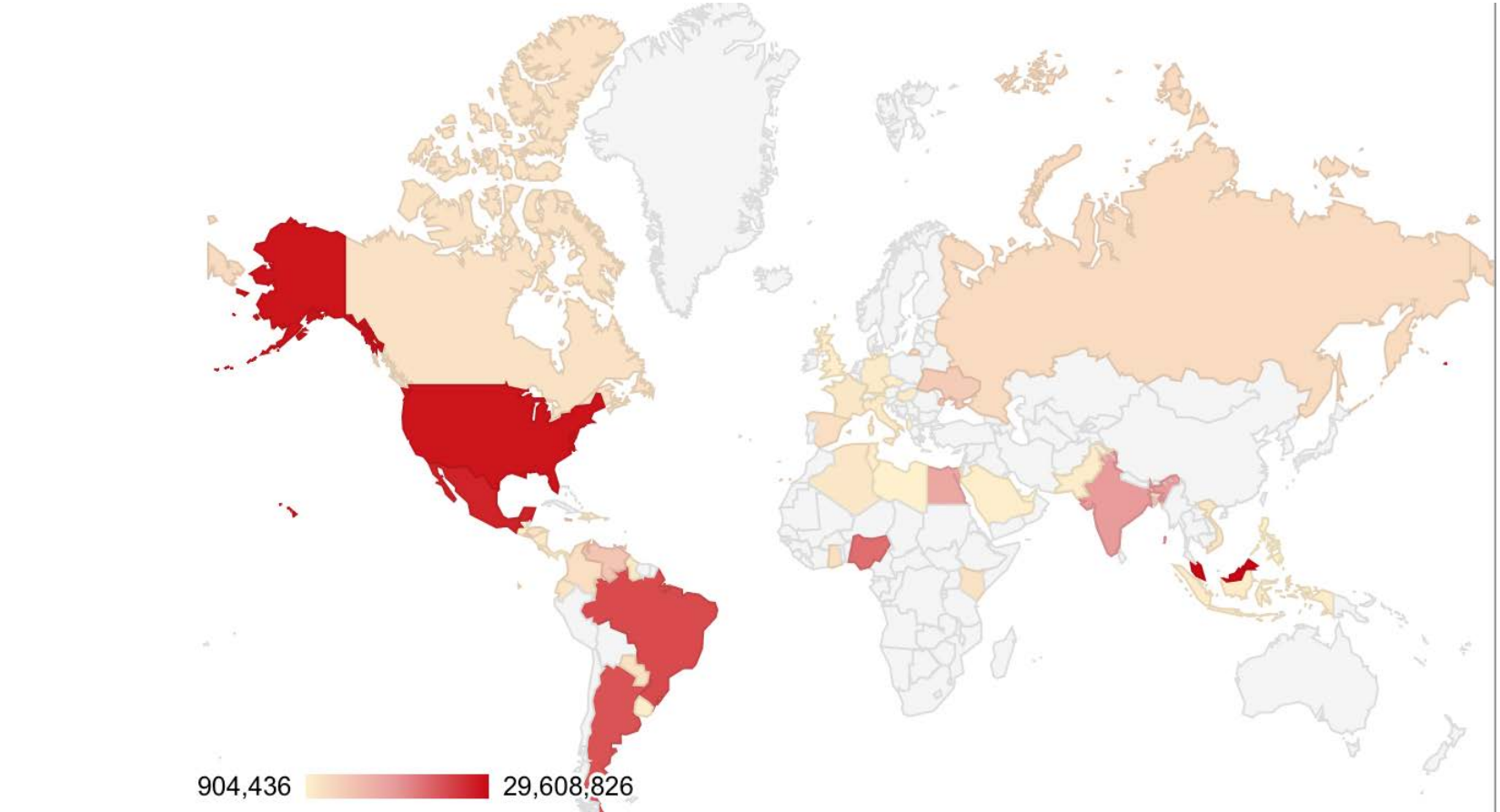
- A lot of devices periodically trying to contact a set of predefined domain names
  - All available except one ( Hosted in China )
- Devices with a active by default “debug” setting
- Traced back to the firmware developer and mobile device retail distributors

# Abandonware - Not just mobile apps

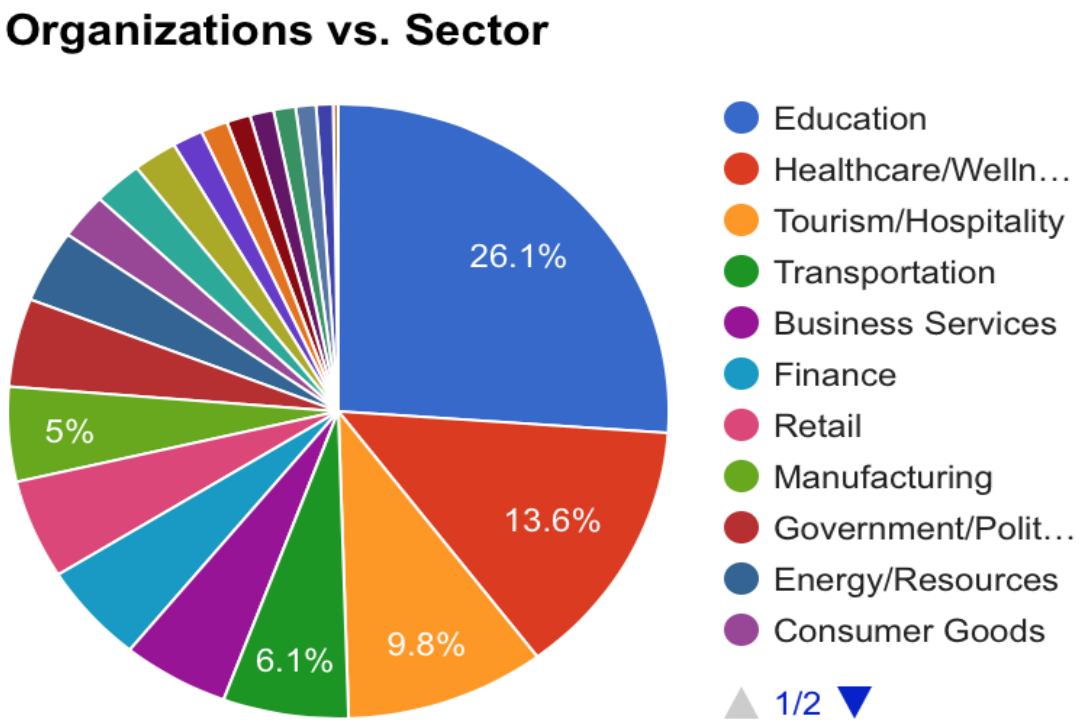
**The Android firmware “incident”** - Yet another strange fish on the net

- Impact:
  - Information leak
  - Update configurations
  - Install applications
  - Execution of arbitrary commands as “root”
  - Not an app, not visible, can’t really “uninstall”
- 7 day time window observations:
  - **322,382,506** Events processed
  - **7,378,303** Unique IP addresses identified

# Android firmware - Geo distribution



# Android firmware - Sector distribution



# Q&A

# Thank You!

joao.gouveia@bitsighttech.com

BITSIGHT

125 CambridgePark Drive, Suite 204
Cambridge, MA. 02140

info@bitsighttech.com