RSA®Conference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

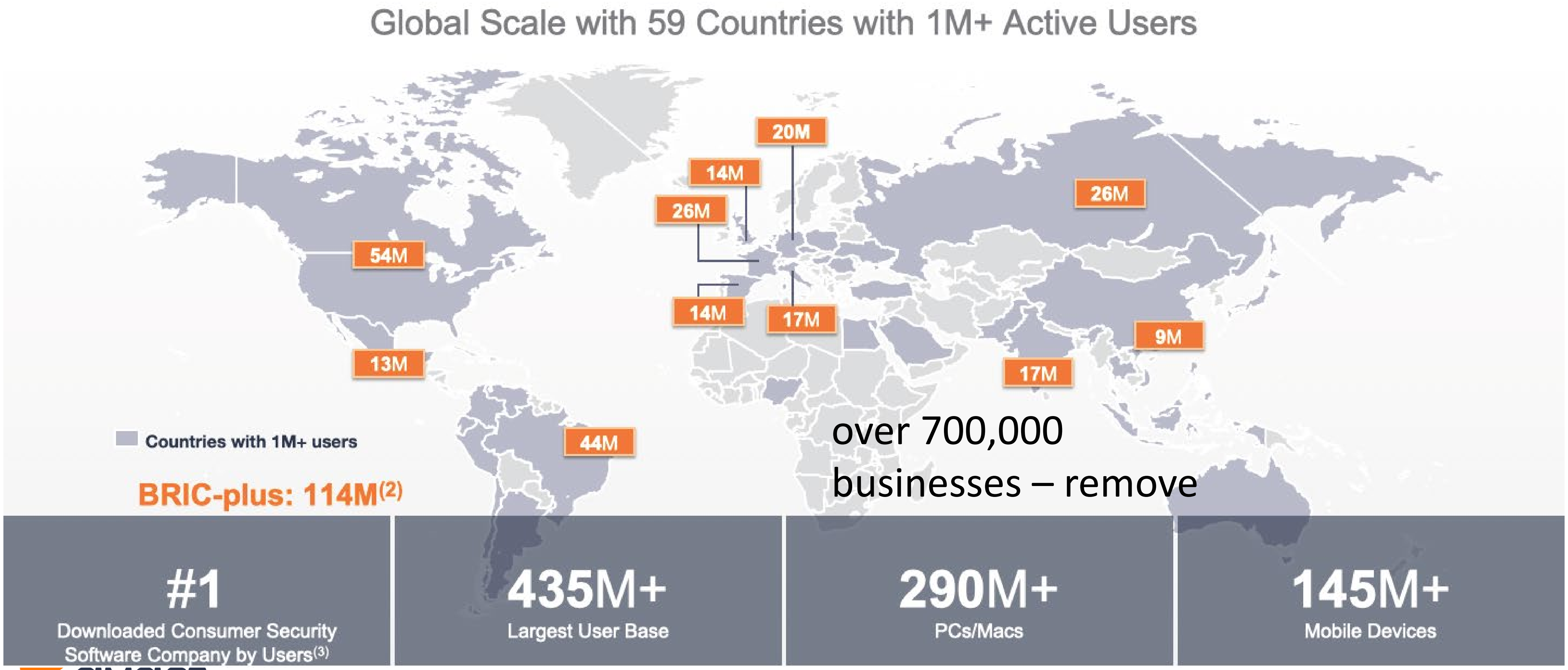
SESSION ID: SBX1-W2

Shadow IoT Hacking the Corporate Environment: Office as the New Smart Home

Ondrej Vlcek

President and Chief Technology Officer
Avast
@avastvlk

World’s largest provider of Consumer Protection, Privacy, and Performance Products



Global Scale with 59 Countries with 1M+ Active Users

▨ Countries with 1M+ users

BRIC-plus: 114M[2]

over 700,000 businesses – remove

#1
Downloaded Consumer Security Software Company by Users[3]

435M+
Largest User Base

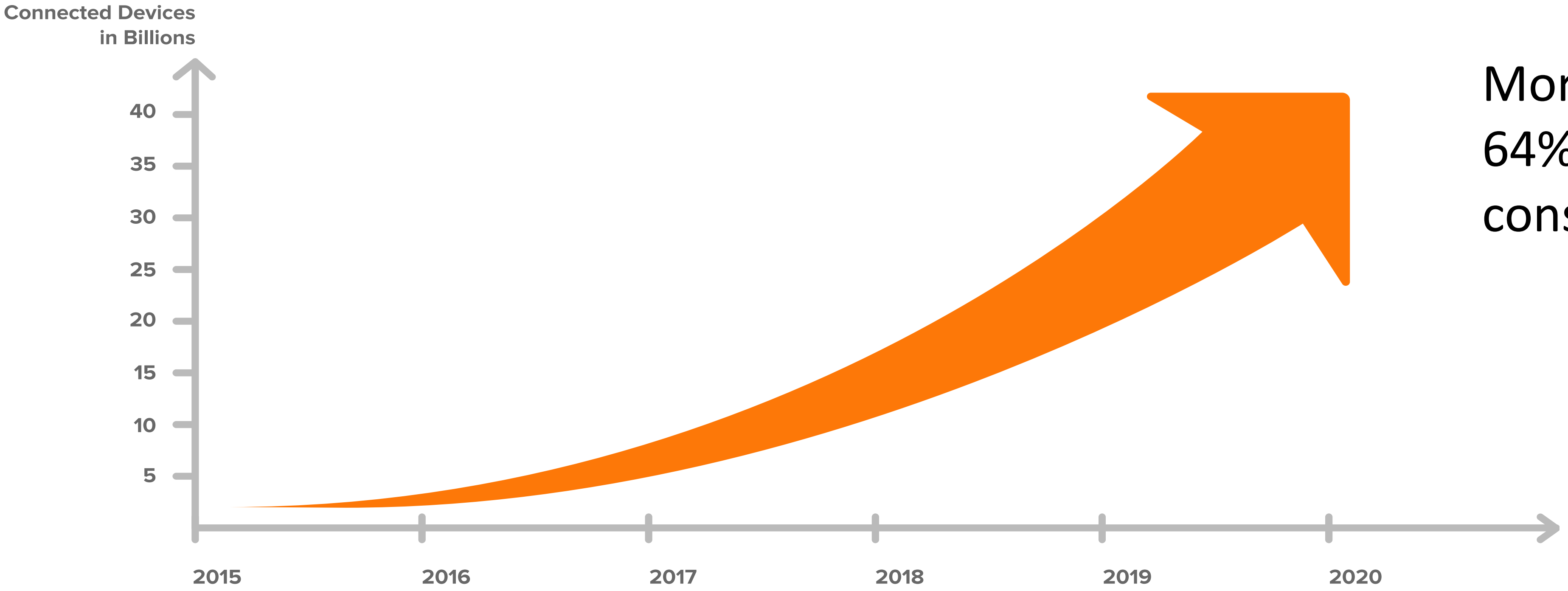
290M+
PCs/Macs

145M+
Mobile Devices

avast

The Number of Connected Devices Is Growing Exponentially

The types of connected devices are expanding broadly



- TVs
- Toys
- Lighting
- Game Consoles

- Home Climate
- Car Infotainment
- Healthcare
- Car Safety

- VR Displays
- Self-Driving Cars
- AR Displays
- Smart Meters

- Delivery Drones
- Personal Wellness / Quantified Self
- Security Sensors

More than 64% are consumer

I would like to work in the ab statistic somewhere in relationship to the chart.

What does the smart home of today look like?

Stanford University

avast

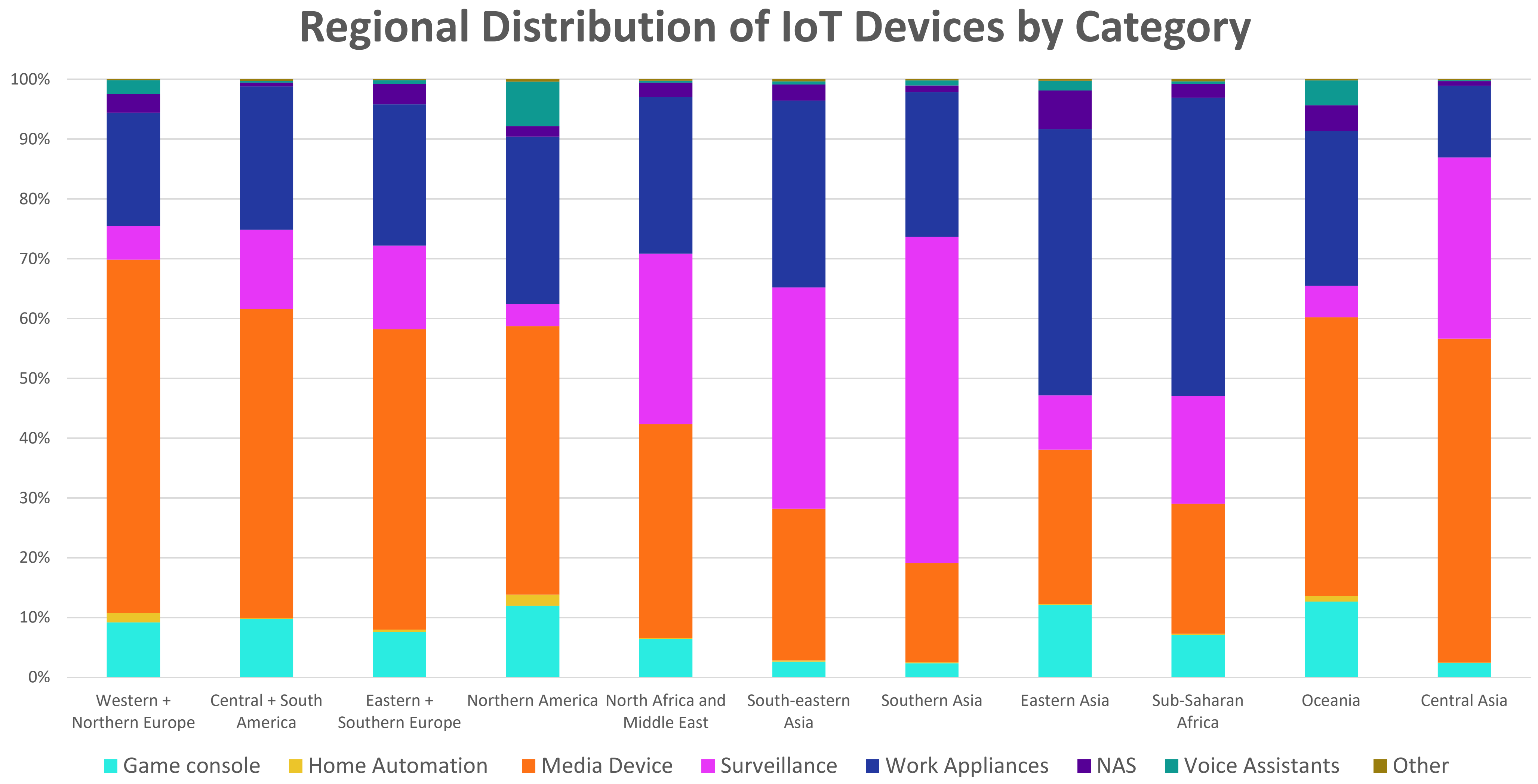
Prof. Zakir Durumeric

Can we make this look pretty with the two logos and a more graphical representation of the two number figures?

Analyzed Avast data for December 2018

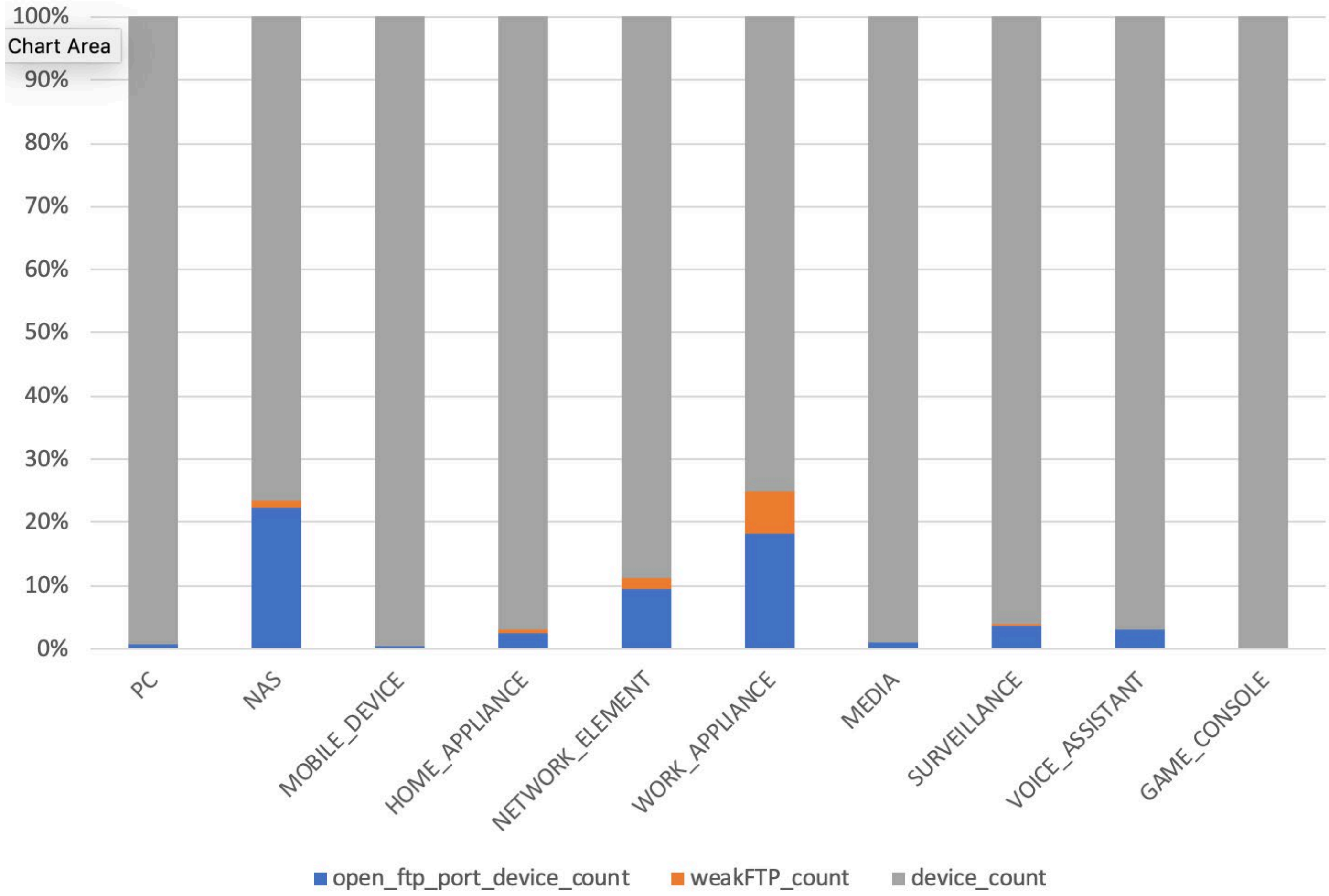
- 15.5M homes
- 83M devices

Device distribution by region



Please edit
the design o
this to your
liking. I have
included the
base figures

Weak credentials and protocols



I have the
background data
on this chart, bu

<Neighboring columns for Telnet and FTP. I can't get excel to do it right now. >

Survey of IT Directors: IoT in the enterprise

mprove
e goal is
the
gned
me
n
on the
k. We
e some
s with
plate if
d to.

35%

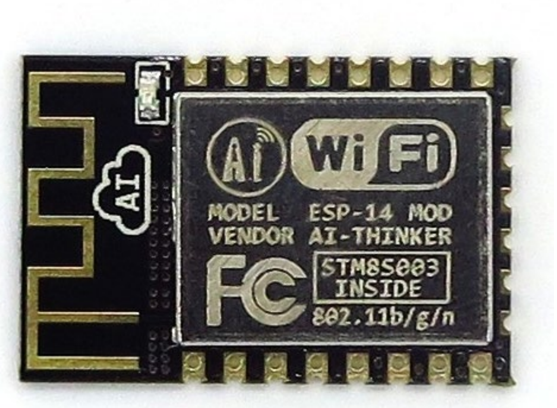
>1,000 Shadow IoT Devices on Corporate Network

39%

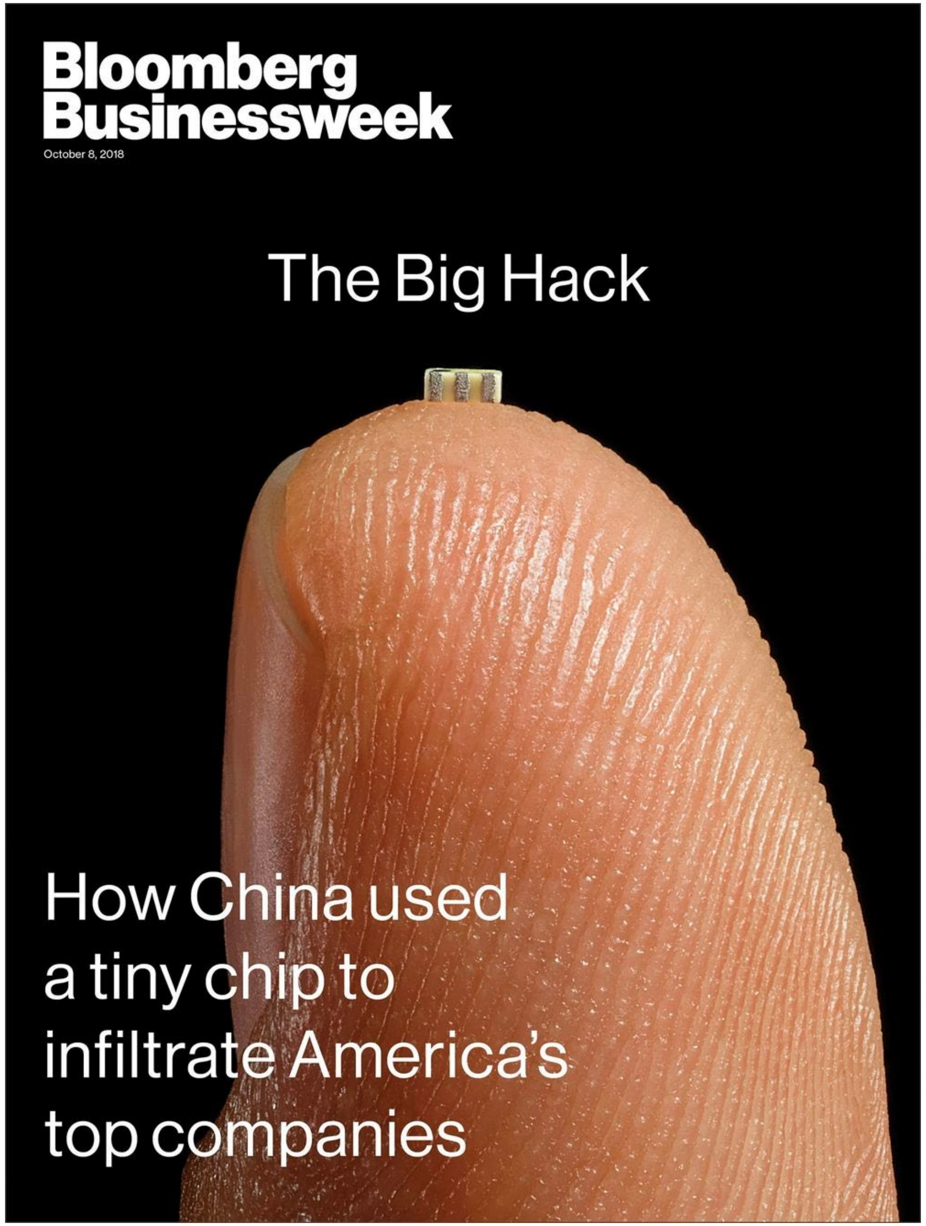
used personal devices connected to the enterprise network

The problem of protecting IoT

Weak Embedded Security | Unprotected Supply Chain | Common Components



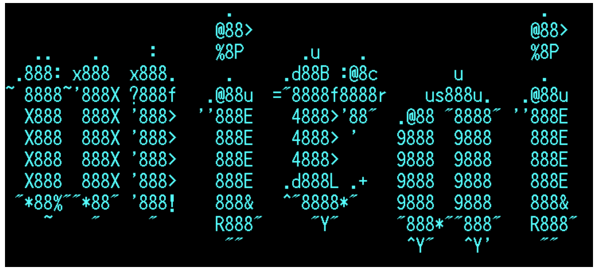
ESP8266


Bloomberg
Businessweek
October 8, 2018
The Big Hack
How China used a tiny chip to infiltrate America's top companies

You don’t have to do this….

There are plenty of ways for rogue devices to get in…

IoT malware getting more and more sophisticated



```
                       .                                 .
                      @88>                              @88>
   ..     .     :      %8P      .u    .                 %8P
 .888: x888  x888.     .     .d88B :@8c        u        .
~ 8888~'888X ?888f   .@88u  ="8888f8888r    us888u.    .@88u
  X888  888X '888>  ''888E    4888>'88"  .@88 "8888"  ''888E
  X888  888X '888>    888E    4888> '    9888  9888     888E
  X888  888X '888>    888E    4888>      9888  9888     888E
  X888  888X '888>    888E   .d888L .+   9888  9888     888E
 "*88%""*88" '888!    888&   ^"8888*"    9888  9888     888&
    ~    "     "      R888"    "Y"       "888*""888"    R888"
                       ""                 ^Y"   ^Y'      ""
```

→

TORII

Early IoT Malware

Single purpose

Focused on DDoS, Cryptomining

Easily spotted and stopped

Evolving IoT Malware

More persistent

Sophisticated obfuscation

Can deliver any kind of malware

Gathers extensive information about the network

Weak Routers at ISPs causing downstream infections

Mikrotik Router Fiasco

- XXX detected infections
- Again, more persistent and sophisticated obfuscation
- Capable of being controlled and repurposed – cryptomining, scanning networks, etc.
- Powerful mesh network of enslaved routers

RSAConference2019

Demo:

Eyes and ears in the enterprise

Recommended Enterprise Approach to IoT security

- Device cataloging
- Network Segmentation
- Network traffic analysis
- Patch management
- Enforcing internal network policies
- Remember, it’s not about the perimeter anymore

Script for Demo

Go to https://docs.google.com/document/d/10bwdHEDJUFbd7BxFk_cBMoyMs8lQSMCGQRvq1RkZh6Y/edit

RSAConference2019

Thank you