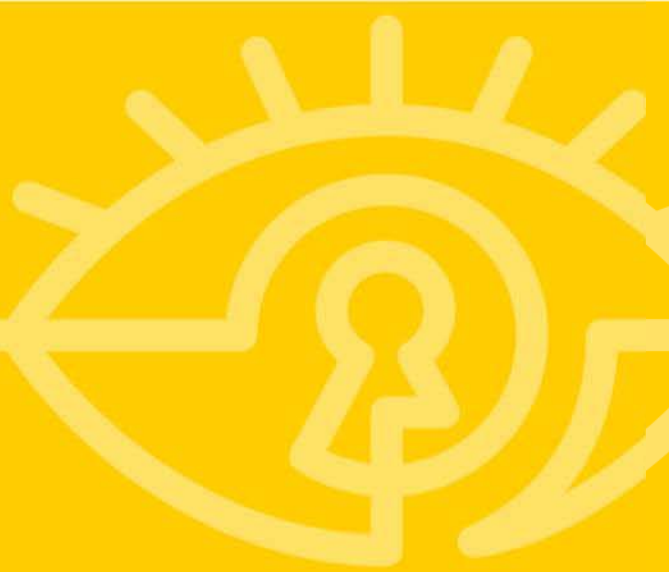
RSA Conference2016
Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

SESSION ID: GPS2-F01

Thingbots: The Future Of Botnets In The Internet Of Things

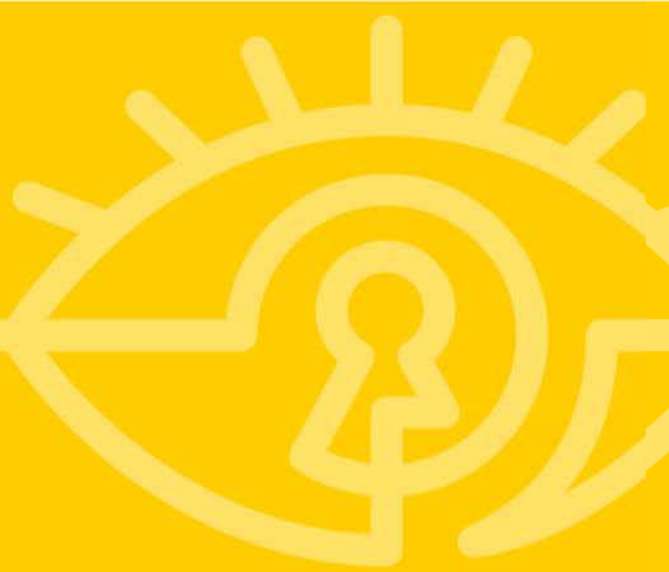
Paul Sabanal
Security Researcher
X-Force Advanced Research
IBM Security
@polsab



Introduction

The Internet of Things is upon us

The Internet of Things is upon us



Thingbots Today

Current state of IoT malware

ars technica

Hackers hijack 300,000-plus wireless routers, make malicious changes *March, 2014*

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

Cryptocurrency mining malware discovered on surveillance DVRs *April, 2014*

CSO

New toolkit seeks routers, Internet of Things for DDoS botnet *September 2014*

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Worm Uses ShellShock to Infect QNAP Network Storage Systems *December 2014*

NETWORKWORLD

Thanks to default passwords, Moose malware may infect Linux-based routers near you soon *May 2015*

engadget

Malware turns hundreds of security cameras into a botnet *October, 2015*

Forbes

Someone Has Hacked 10,000 Home Routers To Make Them More Secure *October 2015*

PCWorld

Android-powered smart TVs targeted by malicious apps *January 2016*

Examples

TheMoon

- Affects Linksys E-series routers
- Exploits an HNAP command injection vulnerability
- First discovered in February 2014

Lizard Stresser

- Booter service used to DDoS Xbox and Playstation networks in January 2015
- Bot is a variant of FGT
- Infects devices running Linux
- Spreads through telnet login using factory default credentials

Moose

- Affects routers running Linux
- Spreads through weak telnet login credentials
- Steals cookies from unencrypted social networking sites traffic
- DNS hijacking

Wifatch

- “The Vigilante Malware”
- Targets devices running Linux
- Spreads through weak telnet login credentials
- Peer to peer C&C
- Disables telnet to prevent other malware out
- Removes known malware

Examples

Carna

- ❑ Anonymous researcher wants to map the entire Internet
- ❑ Infected 420,000 devices to use as scanners
- ❑ Spreads through default or empty telnet login credentials
- ❑ No malicious behavior
- ❑ Prevents Aidra from infecting device

Darlloz

- ❑ Targets routers, cameras, and other devices running Linux
- ❑ Spreads through telnet login
- ❑ Mines for Mincoin and Dogecoin
- ❑ Removes Aidra when found on the device

Aidra

- ❑ Open source
- ❑ Exploits old D-Link router vulnerabilities
- ❑ Telnet login using bot master provided credentials
- ❑ C&C via IRC
- ❑ DDoS attacks

Current state of IoT malware

Devices

mostly routers

some network cameras

a few others

OS

embedded Linux

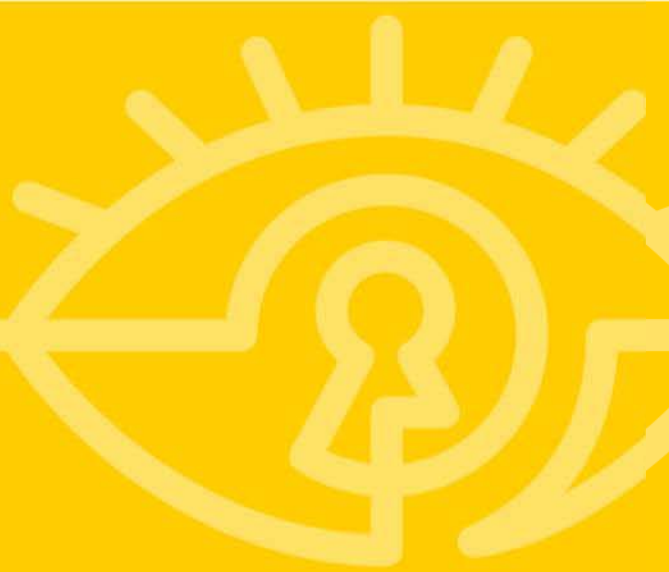
Infection Methods

default credentials

device vulnerabilities

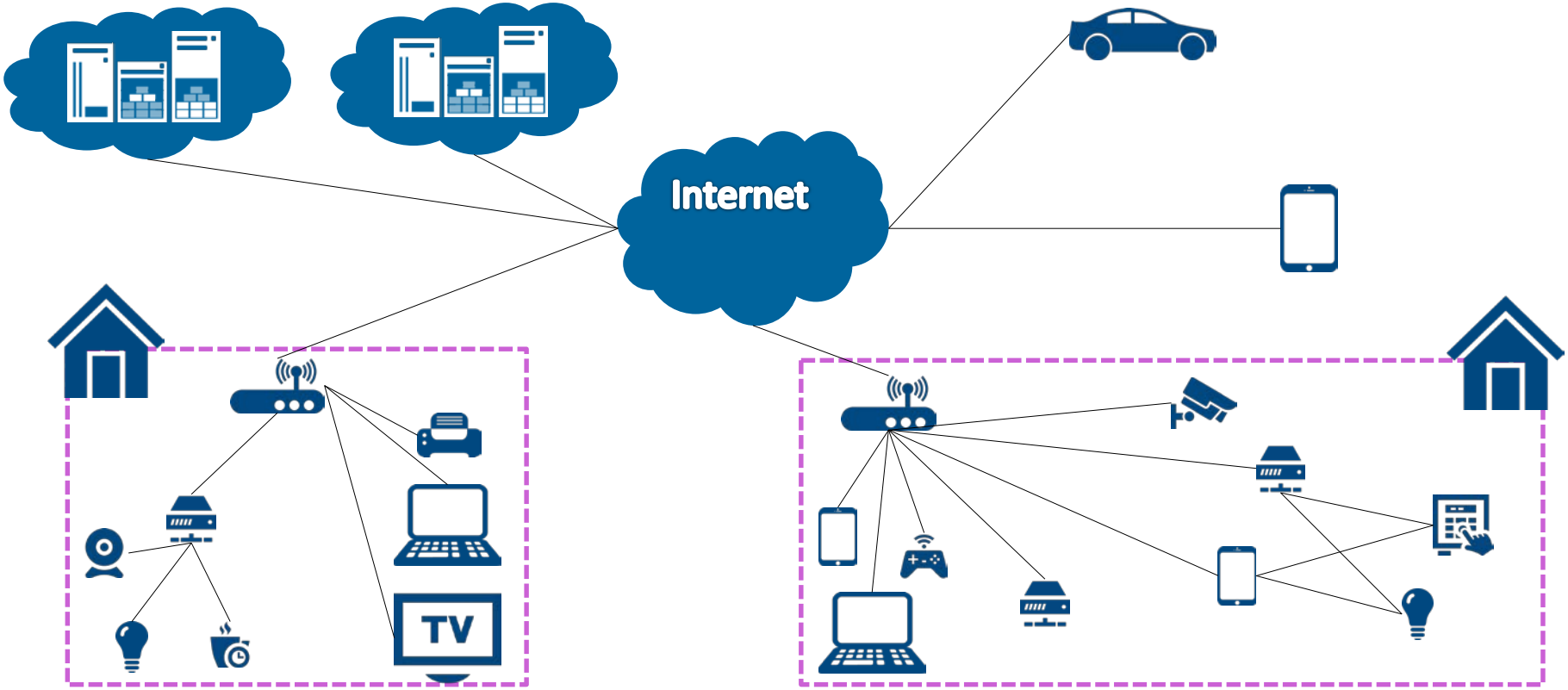
Purpose

DDoS

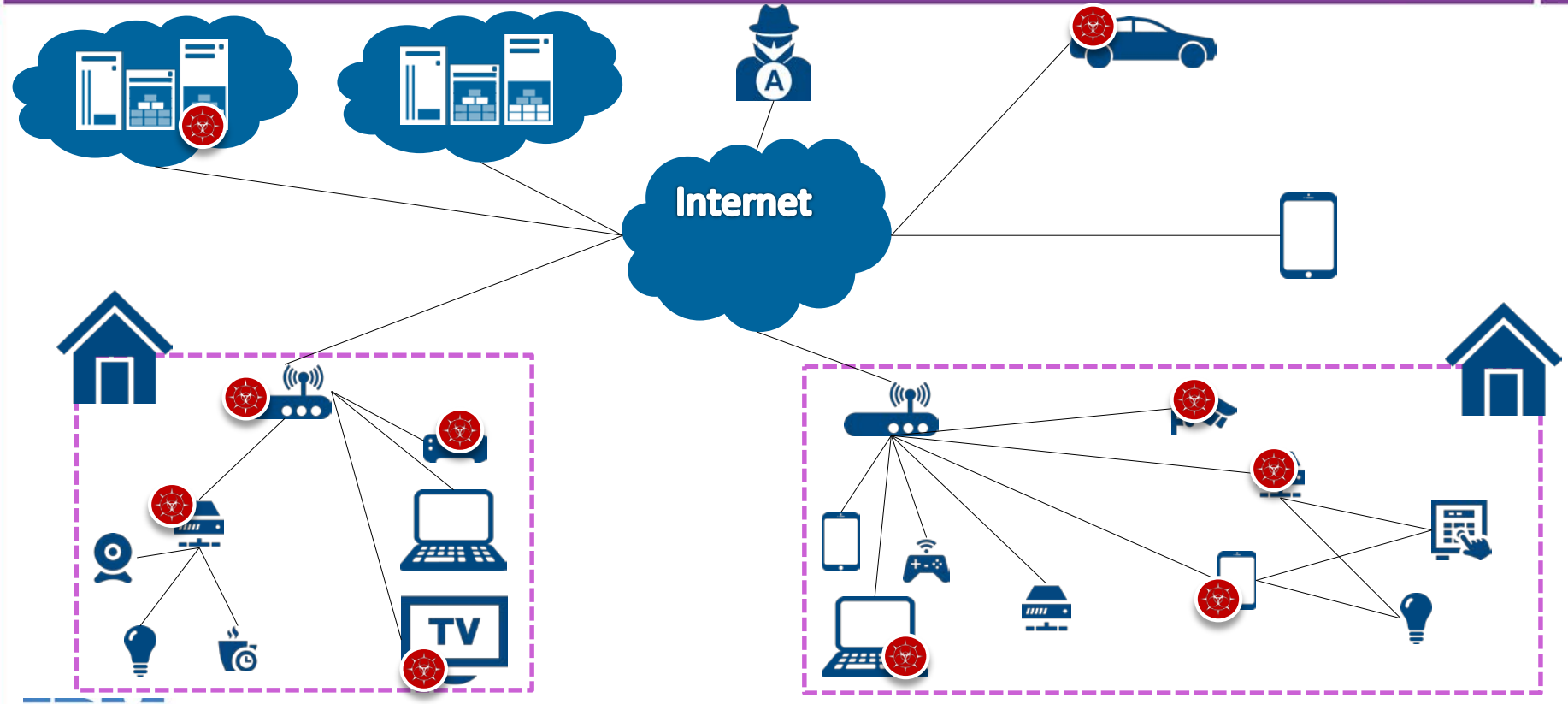


Thingbots Tomorrow

IoT architecture



IoT architecture



Delivery

default credentials

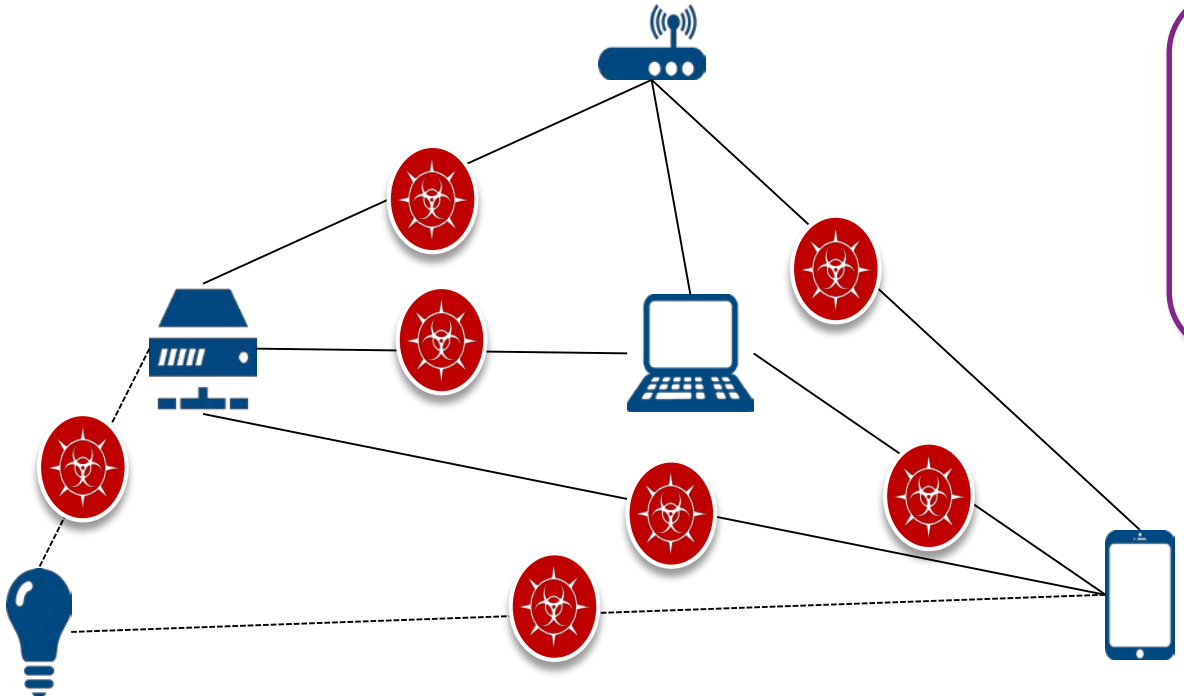
device vulnerability

server compromise

malicious app/plugins

cross device infection

Cross device infection



- Wi-Fi
- Bluetooth
- Zigbee
- RF
- Etc…

Target OSes

Target devices

Command and Control

IRC
HTTP
P2P
social networks
custom protocols

Wi-Fi
Bluetooth
Zigbee
RF
Etc…

dweet.io

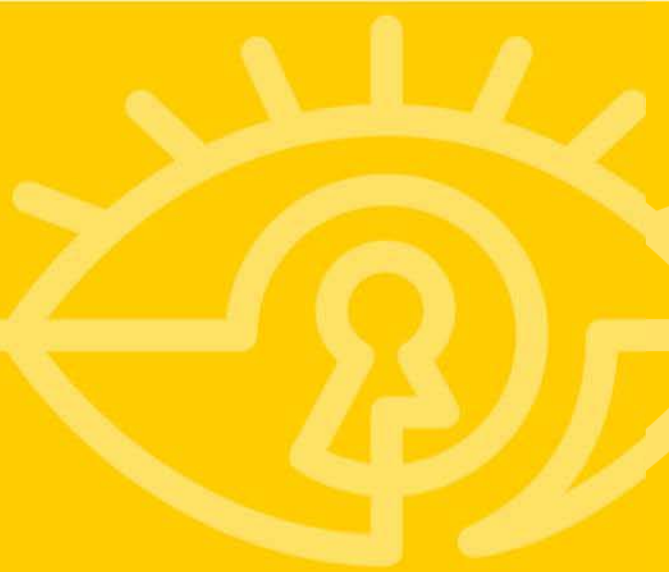
data.sparkfun.com

ThingSpeak

m2m platforms for C&C and data exfiltration

Monetization

- botnet for sale/rent
- spam
- DDoS
- cryptocurrency mining
- click fraud
- ransomware
- data theft



Recommendations

For vendors

secure coding practices

digitally signed firmware

timely updates

consider incorporating intrusion/anomaly detection in hubs/devices

For consumers

standard desktop malware precautions still apply

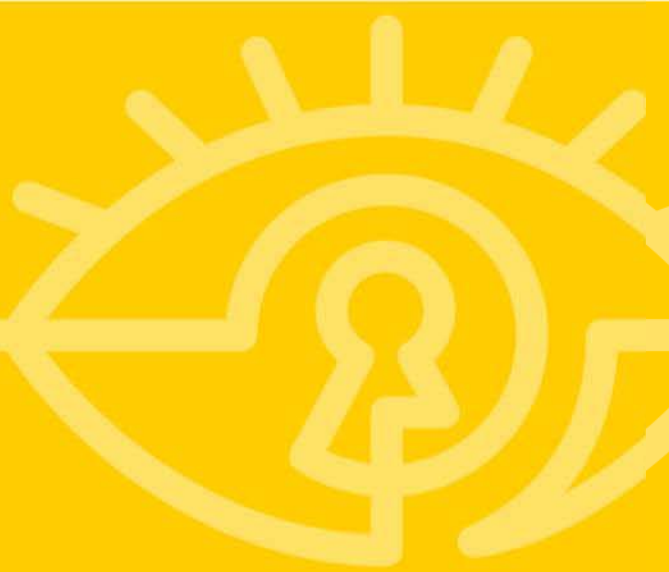
segment your network to minimize lateral infection

change default login credentials

demand more security from vendors

install apps/plugins only from trusted sources

install updates/patches as soon as available



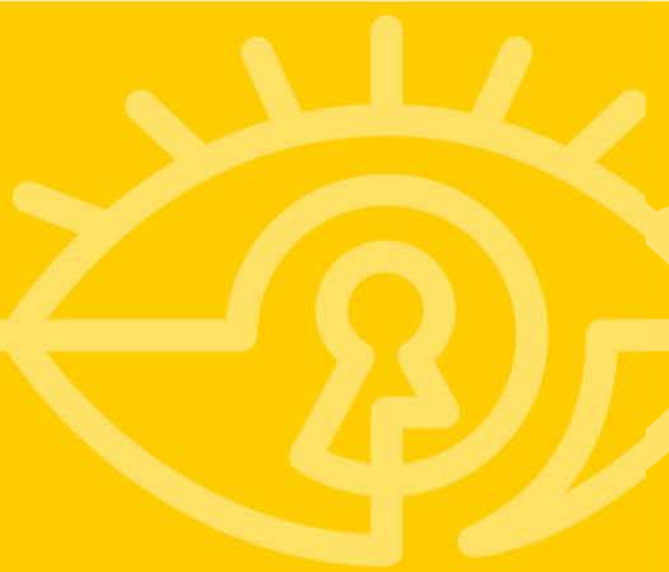
Summary

Summary

thingbots are already here,
and there are more to come

we have yet to see what
they are capable of

vendors, start thinking about security
users, start demanding security



Thank You!

Email:
sabanapm@ph.ibm.com