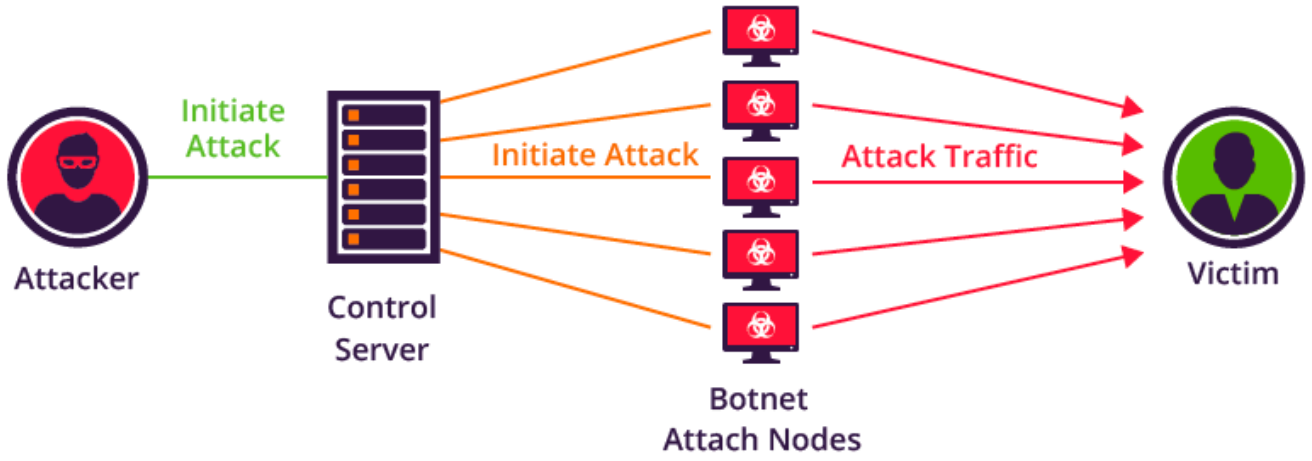
Detecting IoT-based Botnet Attacks

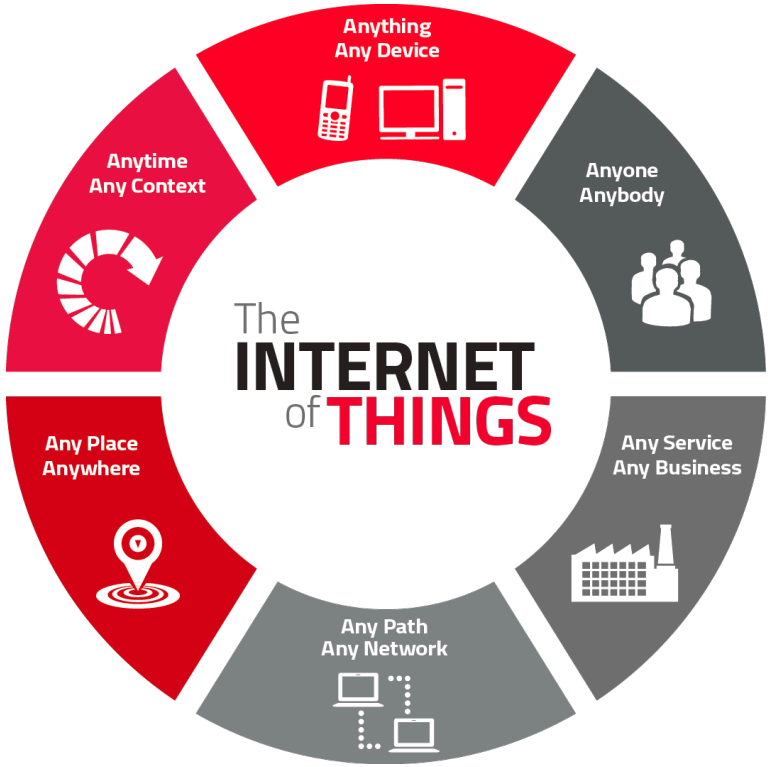
Patrick Routh

Cybersecurity 101

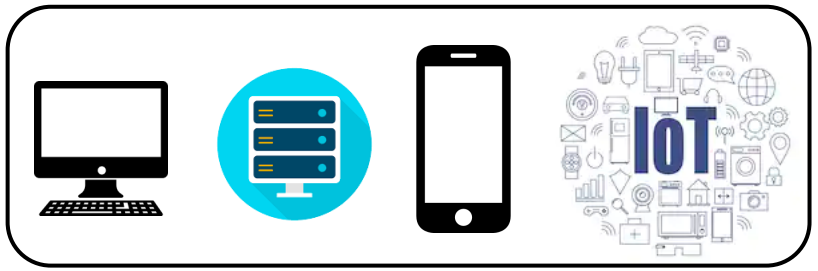
What is a Botnet?



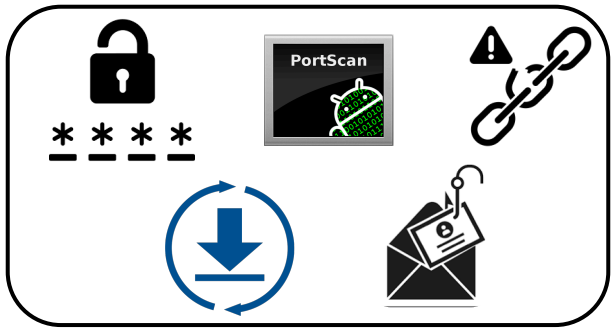
What is the Internet of Things?



What devices are susceptible?

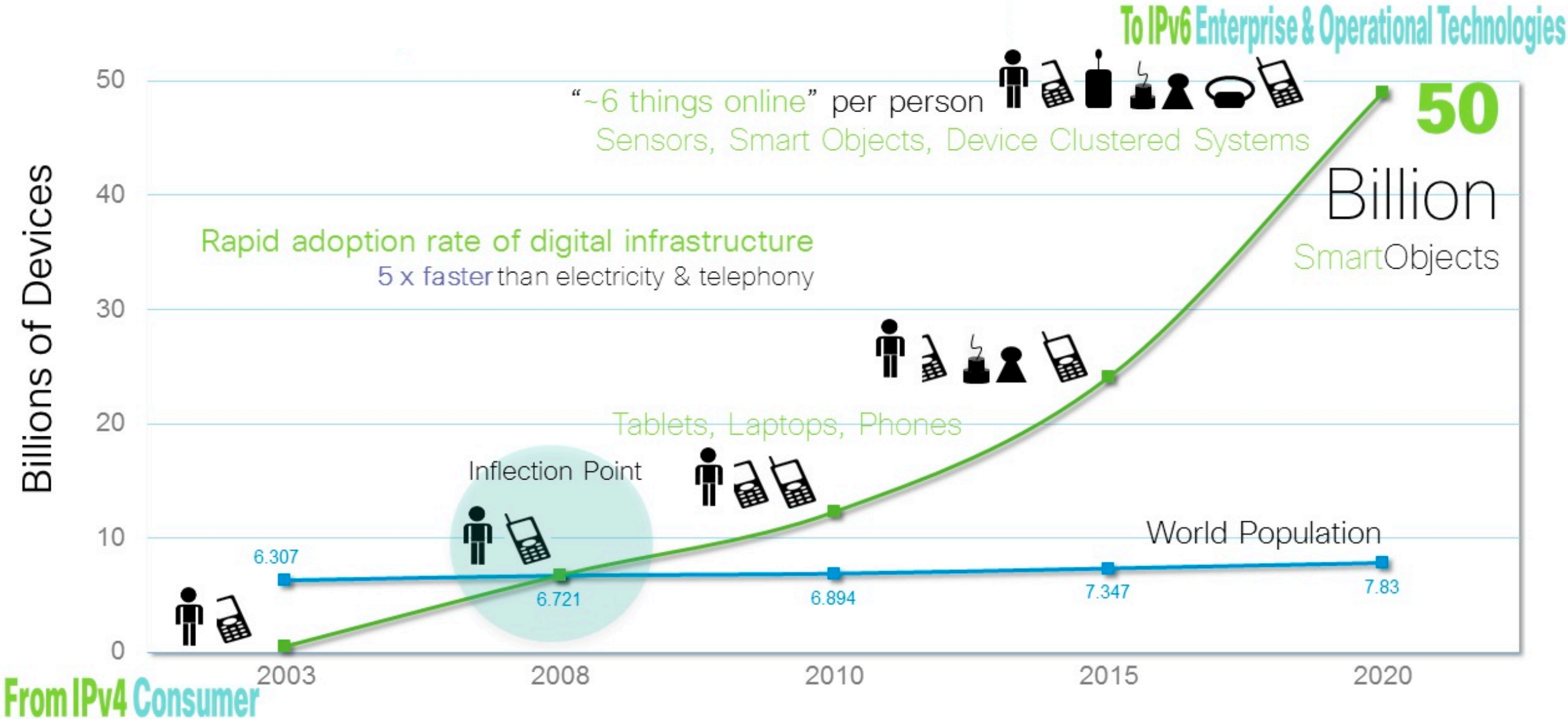


How do botnets spread?



Why are they dangerous?

Projecting the Growth of IoT

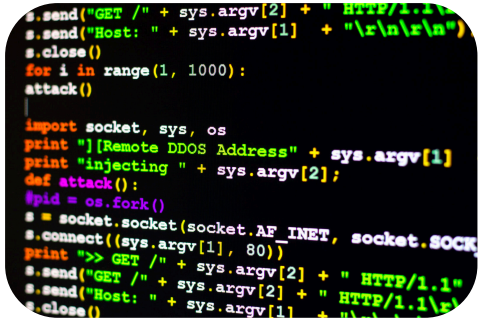


Source: Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf

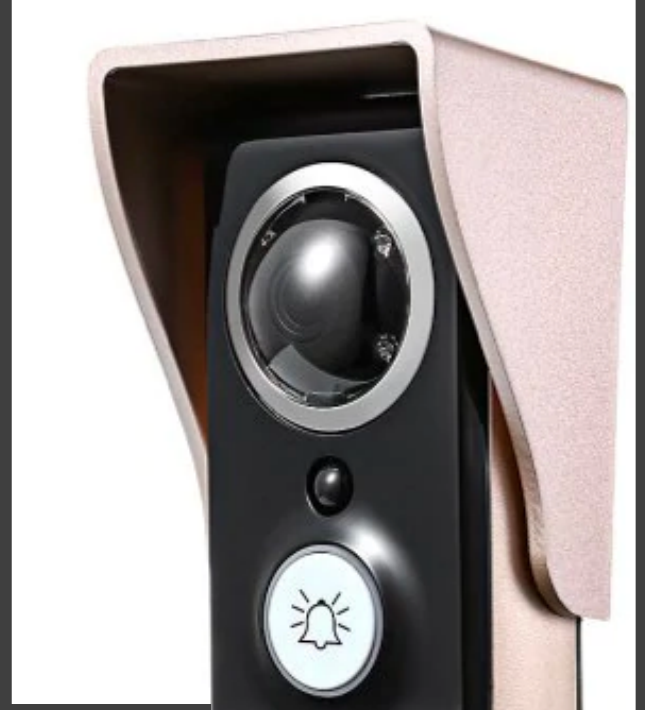
Infamous Botnets

Mirai

BASHLITE



Targeted Devices	Linux-based systems	Linux-based systems
Types of Attacks Launched	DDoS – GRE floods, Water Torture attacks	DDoS
Exploits Leveraged	Open Telnet Ports, default passwords	Shellshock software bug – bash shell
Types of Devices Infected	IoT devices – CCTV Cameras, DVRs Home routers	IoT devices – 96% (cameras and DVRs) Home routers – 4%
Known For	Taking down Internet in Liberia - 2016 DDoS attack on Dyn ISP - 2016	Concentrated attacks on Brazil, Columbia, Taiwan – 2014 Pre-cursor to Mirai – mutations/variants
Propagation Method	Scans Internet for devices running on ARC processor	Exploit devices running BusyBox



IoT Devices

- Provision PT-737 Security Camera
- Provision PT-838 Security Camera
- SimpleHome XCS7-1002 Wi-Fi Security Camera
- SimpleHome XCS7-1003 Outdoor Security Camera
- Philips B120N/10 Wireless Baby Monitor
- Danmini Wi-Fi Video Doorbell
- Ennio CT8501A12 Video Intercom Doorbell
- Ecobee SmartThermostat with Voice Control

Using Machine Learning – to detect botnets

Neural Network Performance Table

Rank	Device Name	Model 1 Acc	Model 1 Loss	Model 2 Acc	Model 2 Loss
1	Ecobee Thermostat	99.92%	0.0044	99.81%	0.0139
2	Philips Baby Monitor	99.91%	0.0044	99.80%	0.0141
3	Provision 838 Security Camera	99.91%	0.0051	99.79%	0.0152
4	Simple Home 1003 Outdoor Security Camera	99.90%	0.0059	99.78%	0.0112
5	Provision 738E Security Camera	99.88%	0.0072	99.77%	0.0170
6	Danmini Doorbell	99.88%	0.0038	99.77%	0.0149
7	SimpleHome 1002 Security Camera	99.87%	0.0052	99.73%	0.0134
8	Ennio Doorbell	99.77%	0.0128	99.81%	0.0142

Simple Home 1003 Outdoor Security Camera – Model 2

Protecting the Internet of Things with Machine Learning

- Remove dependency on host-based security software
- Visibility into machine-to-machine communication
- Real-time detection of malicious traffic
- Automate incident response
- Deliver layered approach to enterprise and personal security