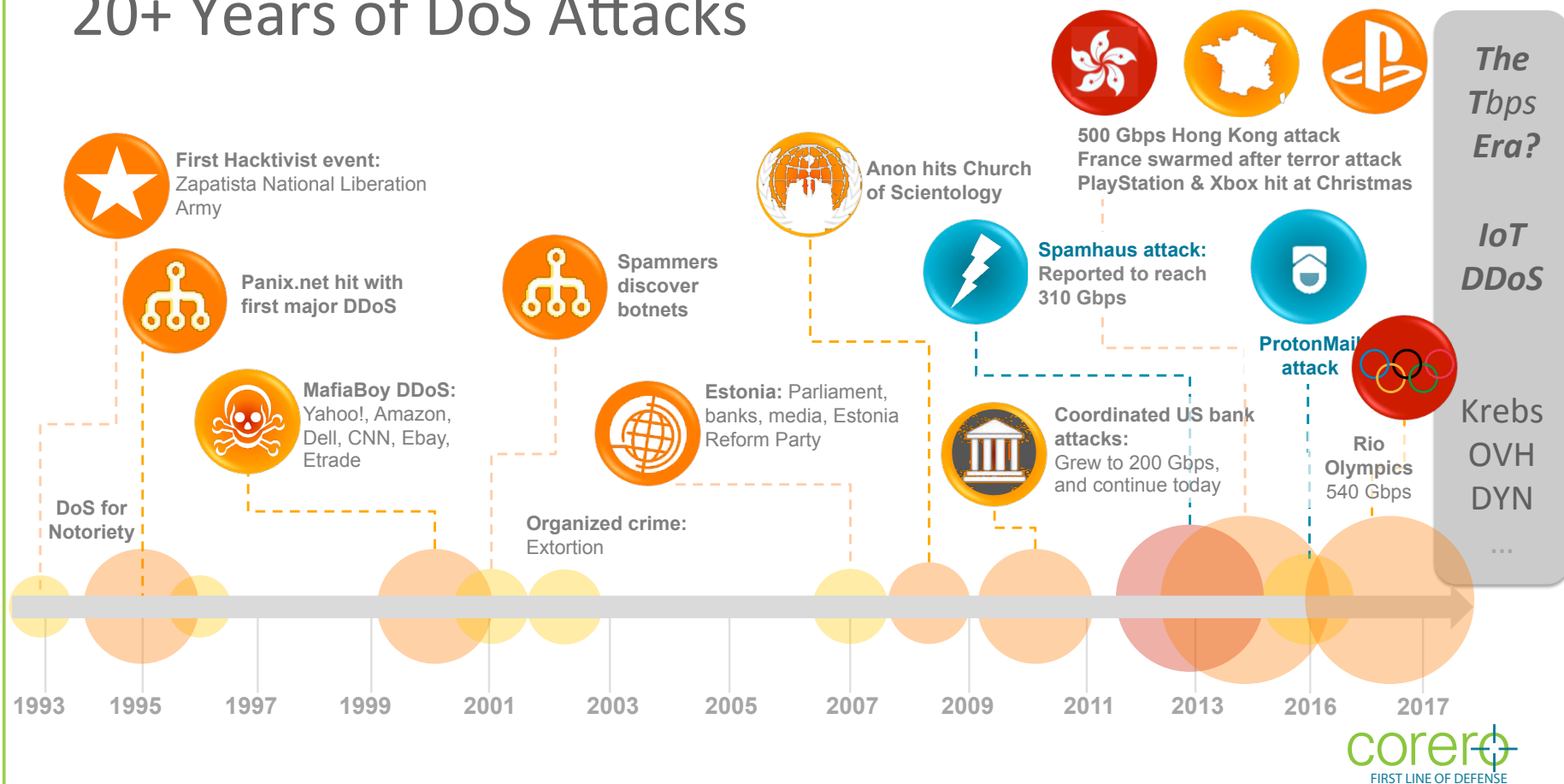


The Security Consideration for IoT

Dave Larson
COO & CTO



20+ Years of DoS Attacks



So what exactly is a 'thing'?

- In the IOT a 'thing' can be many things
 - Security camera, baby monitor, thermostat, DVR, LED light bulb, industrial control device, refrigerator, etc.
- Its what they have in common that's the problem
 - General purpose processor
 - Runs Linux
 - High speed wired/wireless trusted connection
 - Often deployed in default configuration
 - Rarely, if ever, patched or even monitored
 - Little thought given to security architecture



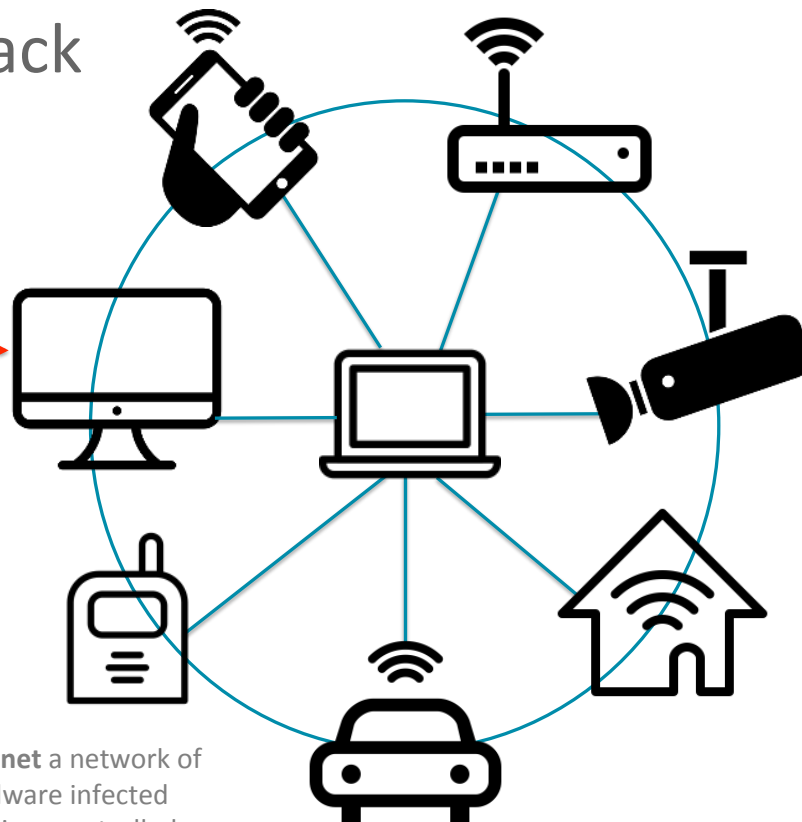
Anatomy of a Botnet DDoS Attack



Attacker installs code that creates a command and control entity that automatically identifies and compromises an army of bots.

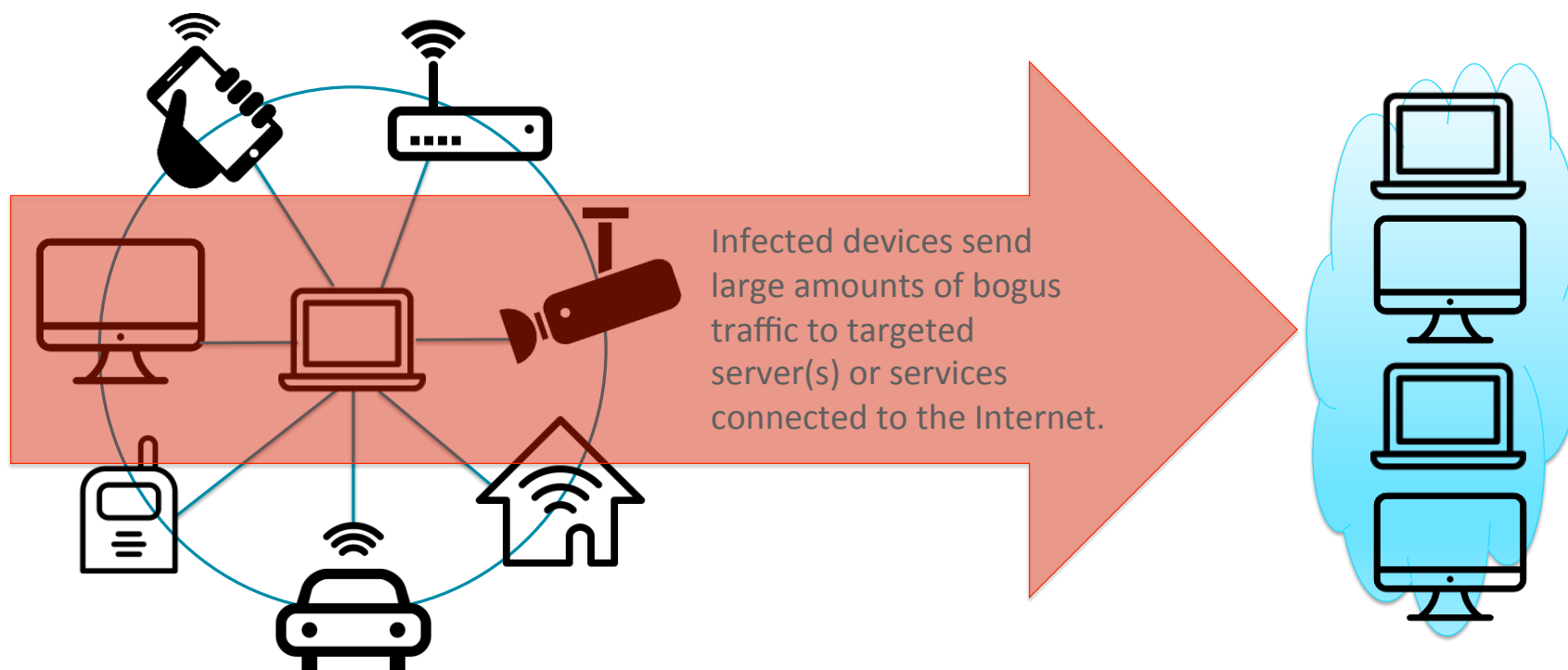


Command and Control Server executes the commands that put the botnet to work.



Botnet a network of malware infected devices controlled remotely by the attacker.

Anatomy of a Botnet DDoS Attack



DDoS always evolving - “IoT” ups the challenge

- Gartner, Inc. forecasts that Internet connected things will reach 20.8 billion by 2020.
- Mirai code made available in early Oct.— malware spreads to devices with factory default or hard-coded usernames and passwords
- Countless attack vectors and attack types out in the wild - Newly discovered CLDAP vector with up to 55x amplification factor
- New techniques, combination attacks, DDoS for hire services coupled with unlimited motivations create a volatile DDoS landscape

Friend or Foe?



Community Responsibility



The Carriers themselves must do more to enable 'clean pipe' to their downstream subscribers—cleaning up attack traffic as well as ensuring that compromised devices on their access network are quickly identified and remediated



Device Manufacturers must put security measures in place. No device should connect to the Internet 'out of the box'



Otherwise we will have government legislation forcing Carriers and Manufactures of IoT devices alike to work toward eliminating the problem

New Breed of Bigger 'Surgical' DDoS Attacks

84%

OF ATTACKS ARE
LESS THAN 10
MINUTES

AVERAGE DURATION OF DDoS ATTACK ATTEMPTS Q1-Q2 2015



Minutes	Volume
0-5	71.6%
6-10	12.6%
11-20	4.2%
21-30	7.0%
31-60	2.2%
>60	2.4%

AVERAGE SIZE OF DDoS ATTACK ATTEMPTS Q1-Q2 2015



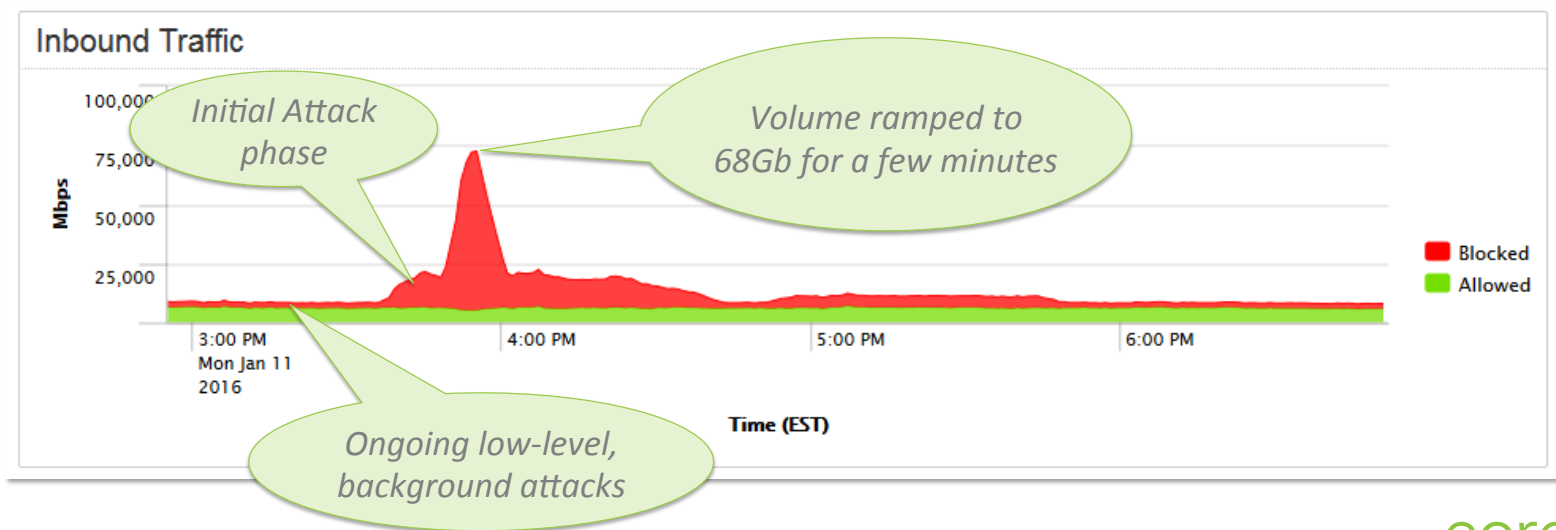
Size	Volume
<1G	93.0%
1G-5G	5.4%
5G-10G	1.3%
>10G	.3%

1.6%

OF ATTACKS ARE
GREATER
THAN 5 Gbps

Sophisticated Multi-Layered Attacks

- Enough volume to cripple target infrastructure or destination
- Advanced DoS attacks crafted to avoid detection
- Short durations avoid legacy DDoS scrubbing mitigation techniques (TTM)






DDoS Protection Recommendations

1. Determine Where to Protect from DDoS

- Defeating DDoS with an always-on deployment at the network edge, removes the threat from your environment
- Legacy approach to mitigation cannot keep up with the evolving threat landscape – (TTM) Time To Mitigation and the scale of attacks (need to inspect every packet)
- New approach, protecting your customer as well as your infrastructure, allows you the provider, to monetize the service and uplift existing services revenue

 The image part with relationship ID rid3 was not found in the file.

2. Choose the right DDoS Protection Service Strategy

- Test solutions for time to mitigation, performance capability, scalability across your network, and automatic security coverage.
- Analytics to ensure you can show the value to your customers to meet their requirements



Thank You!

Dave Larson

Dave.Larson@Corero.com

