ARBOR® NETWORKS

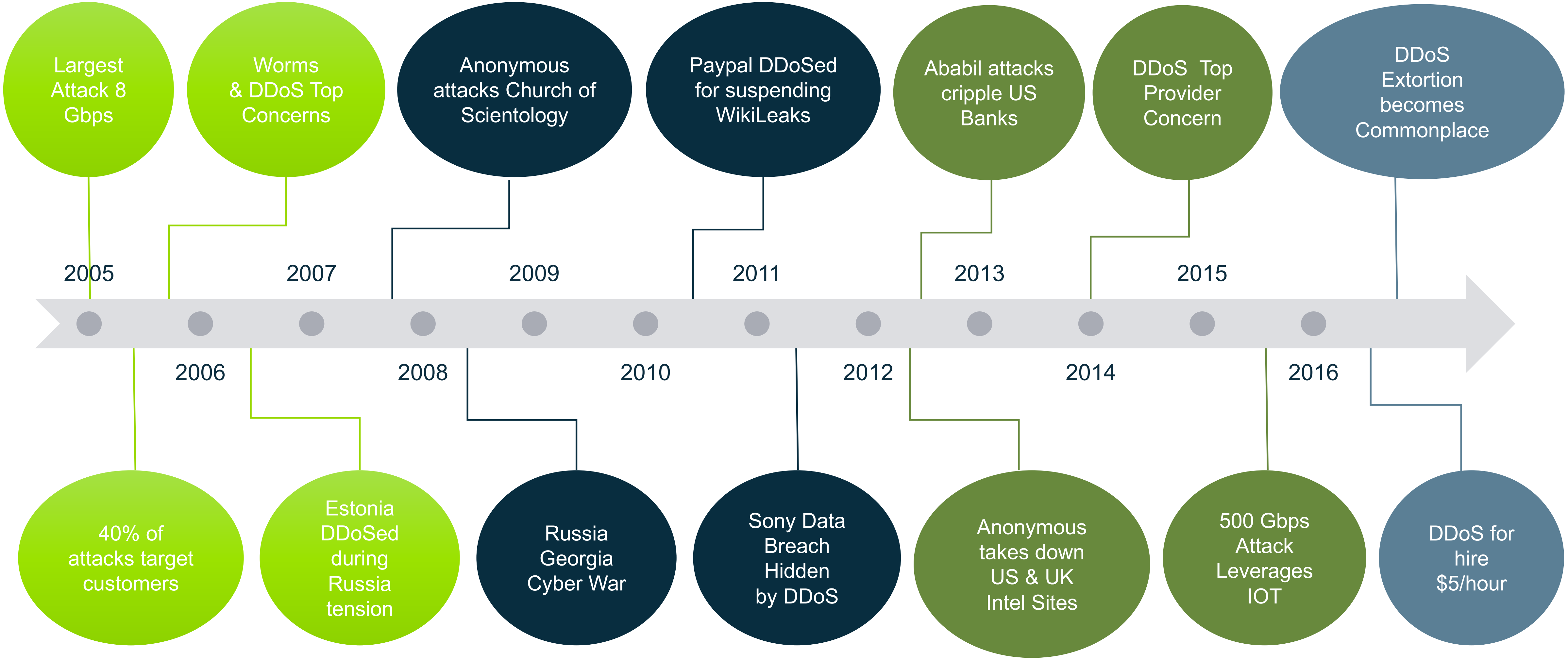
The Security Division of NETSCOUT

Surviving the Inside DDoS attack

Are you ready for the next evolution in DDoS attacks?

C F Chui,
Principal Security Technologist

The Long History of DDoS…



Largest Attack 8 Gbps

Worms & DDoS Top Concerns

Anonymous attacks Church of Scientology

Paypal DDoSed for suspending WikiLeaks

Ababil attacks cripple US Banks

DDoS Top Provider Concern

DDoS Extortion becomes Commonplace

2005

2007

2009

2011

2013

2015

2006

2008

2010

2012

2014

2016

40% of attacks target customers

Estonia DDoSed during Russia tension

Russia Georgia Cyber War

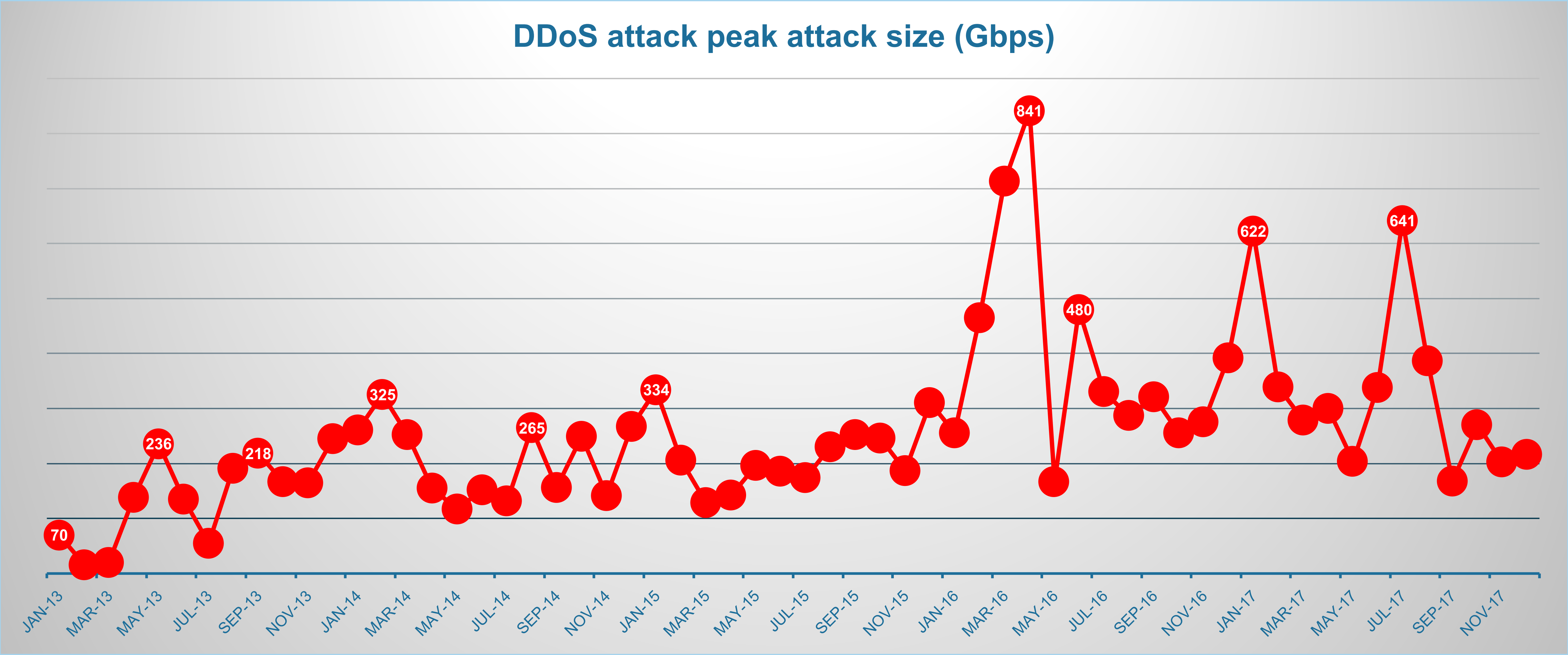
Sony Data Breach Hidden by DDoS

Anonymous takes down US & UK Intel Sites

500 Gbps Attack Leverages IOT

DDoS for hire $5/hour

DDoS: Size getting bigger and bigger

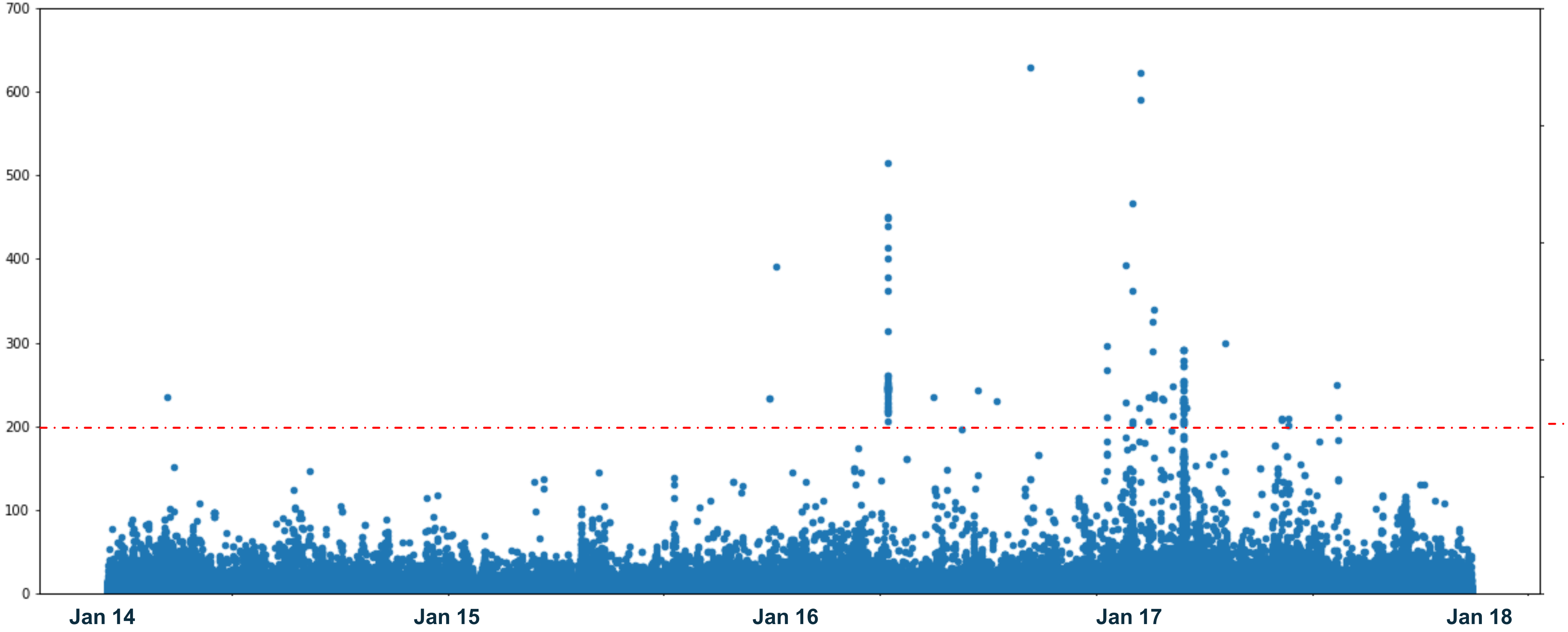


ARBOR NETWORKS

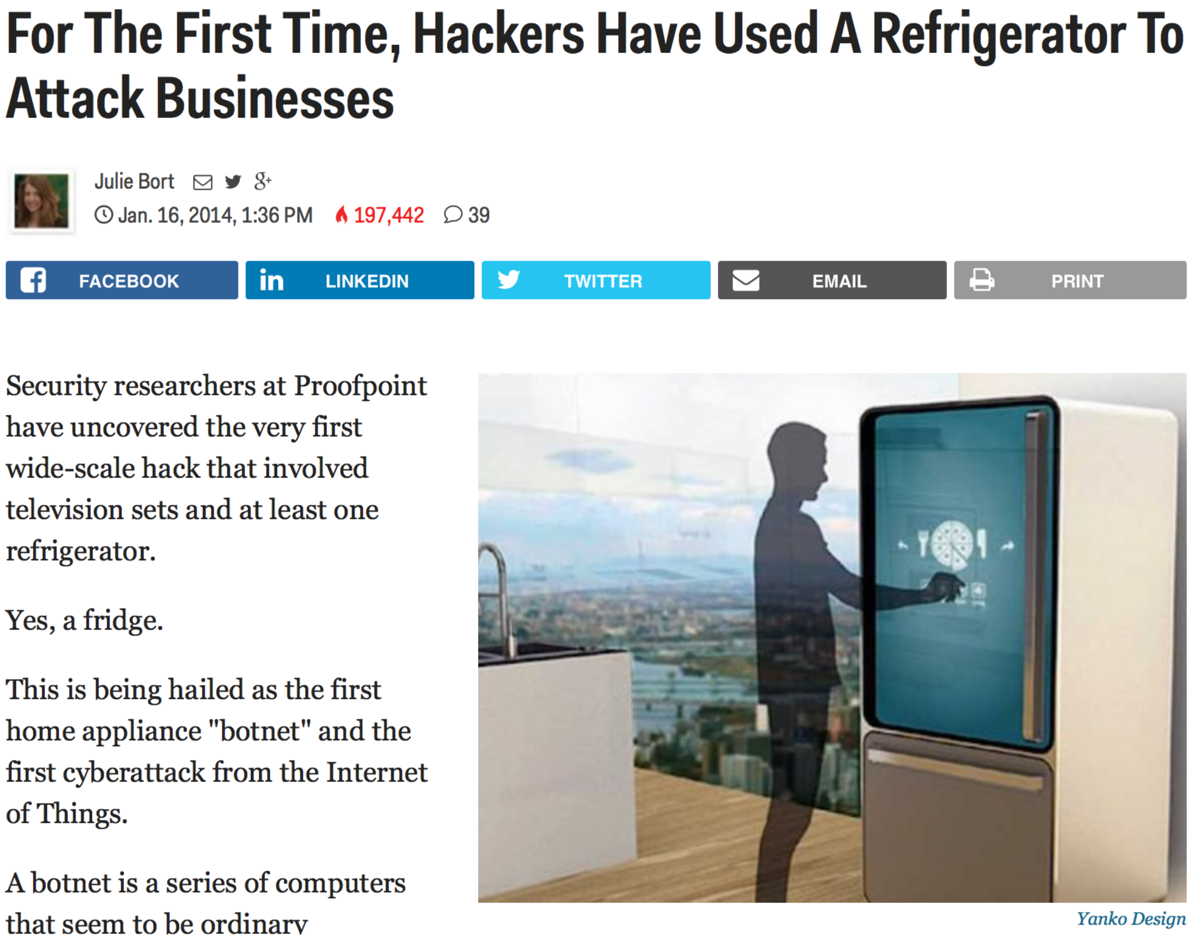
DDoS: APAC perspective

APAC attacks between 2014 to 2017

Lot more attacks over 200 Gbps



Internet of Things



For The First Time, Hackers Have Used A Refrigerator To Attack Businesses

Julie Bort

Jan. 16, 2014, 1:36 PM 197,442 39

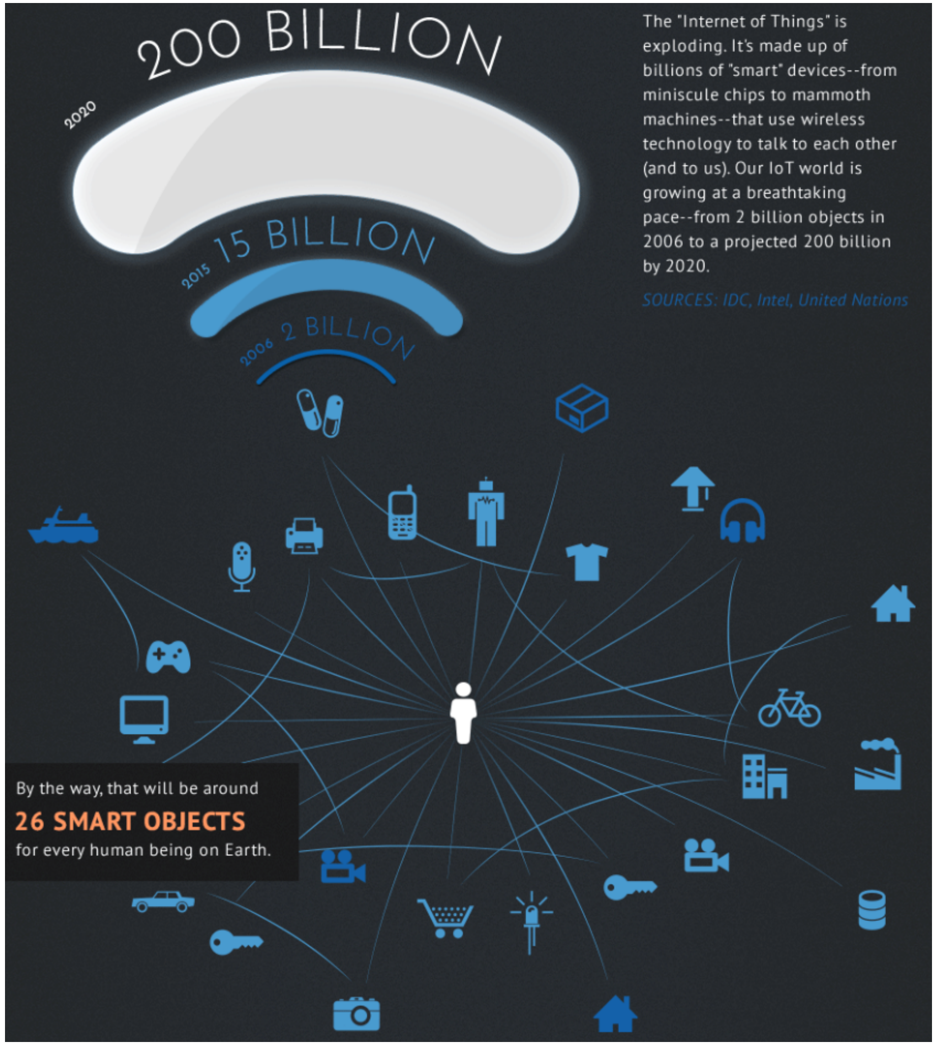
Security researchers at Proofpoint have uncovered the very first wide-scale hack that involved television sets and at least one refrigerator.

Yes, a fridge.

This is being hailed as the first home appliance "botnet" and the first cyberattack from the Internet of Things.

A botnet is a series of computers that seem to be ordinary

Yanko Design



The "Internet of Things" is exploding. It's made up of billions of "smart" devices--from miniscule chips to mammoth machines--that use wireless technology to talk to each other (and to us). Our IoT world is growing at a breathtaking pace--from 2 billion objects in 2006 to a projected 200 billion by 2020.

SOURCES: IDC, Intel, United Nations

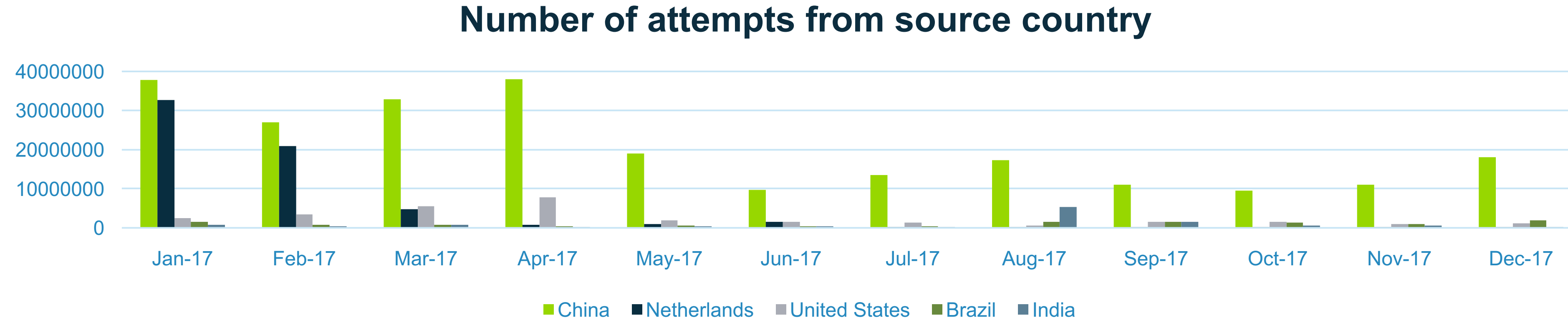
By the way, that will be around **26 SMART OBJECTS** for every human being on Earth.

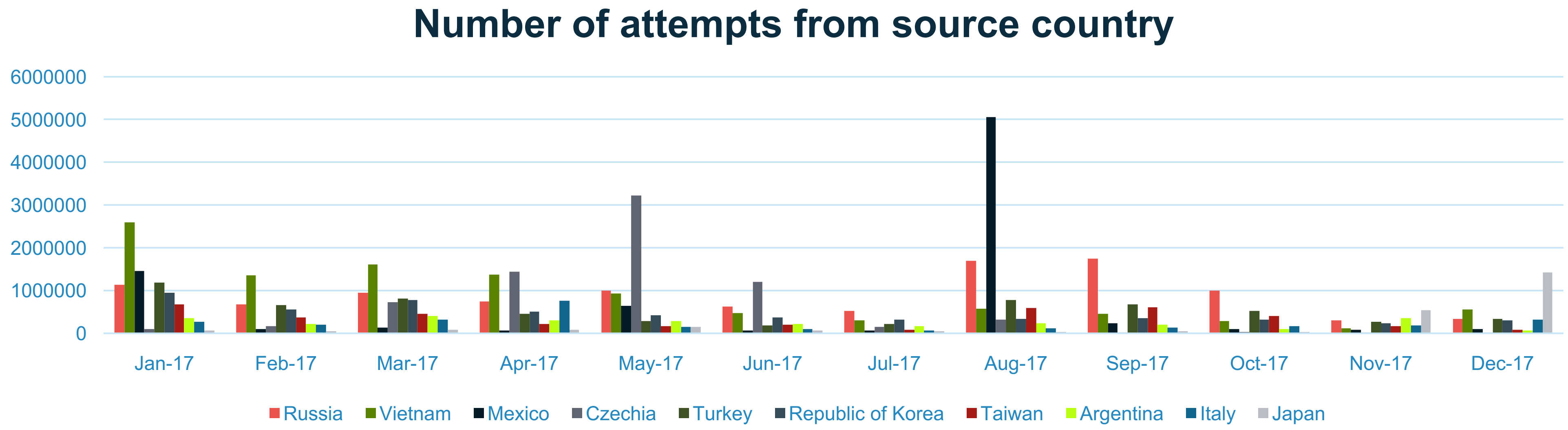
Internet of Things

- More and more low-cost devices being pushed to the web.
- Safety and security taking a back seat.
- Devices that won’t or can’t be patched.
- Enslaved in bot armies through password guessing.
- We need to think about these devices as populations with yield.
- LizardStressor is sourced predominately from web cams.

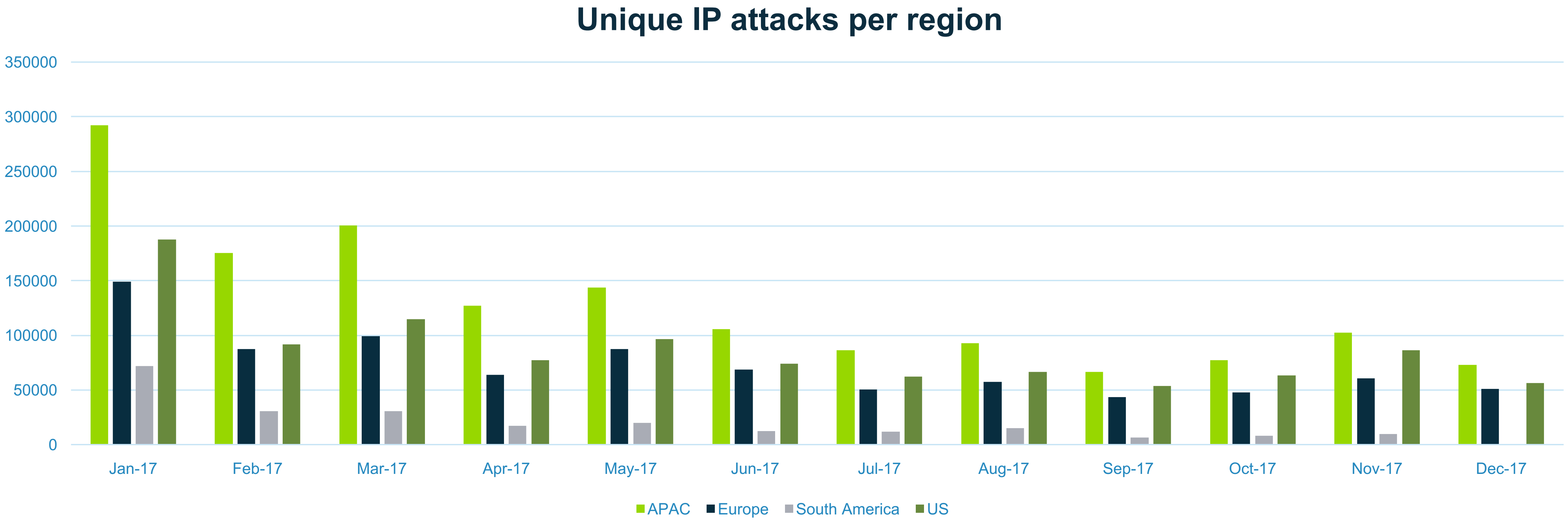
ATLAS Mirai botnet tracking

Country	Count
China	245462847
Netherlands	62241384
United States	29654466
Brazil	12187150
India	11554665
Russia	10734267
Vietnam	10652530
Mexico	8097308
Czechia	7408988
Turkey	6371020
Republic of Korea	5449569
Taiwan	4030567
Argentina	2892572
Italy	2772612
Japan	2622469





ATLAS Mirai botnet tracking



WINDOWS-BASED IoT INFECTION

Background

- Desktop malware spreading multi-platform malware is not new
- Increasingly common technique amongst both targeted malware and crimeware, primarily focusing on mobile devices
  - HackingTeam RCS
  - WireLurker
  - DualToy
  - “BackStab” campaign
- Banking trojans will also target mobile devices to steal 2FA / SMS authorization codes
  - May consist of a side-load installation or tricking a user to click a link on their phone
- IOT devices present a new and ripe infection vector
  - “Windows Mirai” is the first known multi-platform trojan to target IoT devices for infection

“Windows Mirai”

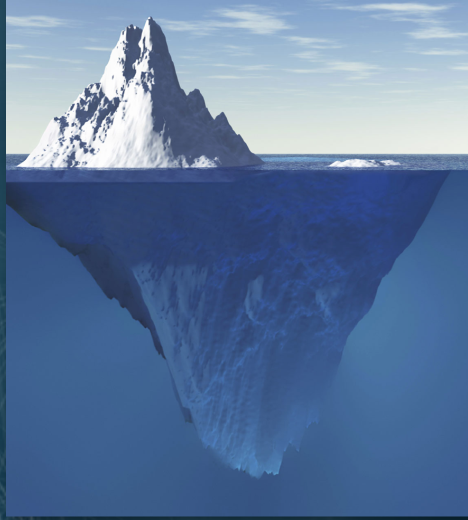
- Initially reported on in early 2017 by PAN
  - Later reported on by multiple organizations
- Not truly a Windows version of Mirai, spread other Linux / IoT malware previously
- Discovered samples dating back to at least March 2016
  - Earliest seen version by ASERT is 1.0.0.2 which was used to spread a Linux SOCKS Trojan
  - Latest known version is 1.0.0.7
- Earlier versions discovered via re-used PE property names
  - Properties combined with recognizable network traffic helped to discover the early versions of the trojan
- Appears to be Chinese in origin, not nation-state related

WM Scanning & Spreading

- Spreads to Windows by
  - Brute-forcing MySQL and MSSQL credentials and injecting stored procedure calls which will download and install the Trojan
  - Also attacks RDP (not in early versions) and WMI

- Spreads to Linux / IoT via
  - Brute-force attacks against Telnet and SSH
    - Use ‘wget’ or ‘tftp’ to download IoT malware loader
    - Newer versions can also echo the loader stored as a resource in the PE file
  - Not currently known to use any IoT exploits to spread like other Mirai variants

IMPLICATIONS & CONSEQUENCES



Implications & Potential Consequences

- **The Zombie horde**

  A single infected Windows computer has now the capability to infect and subvert the ”innocent” IoT population into zombies, all under the control of the attacker.

Game of Thrones 2011

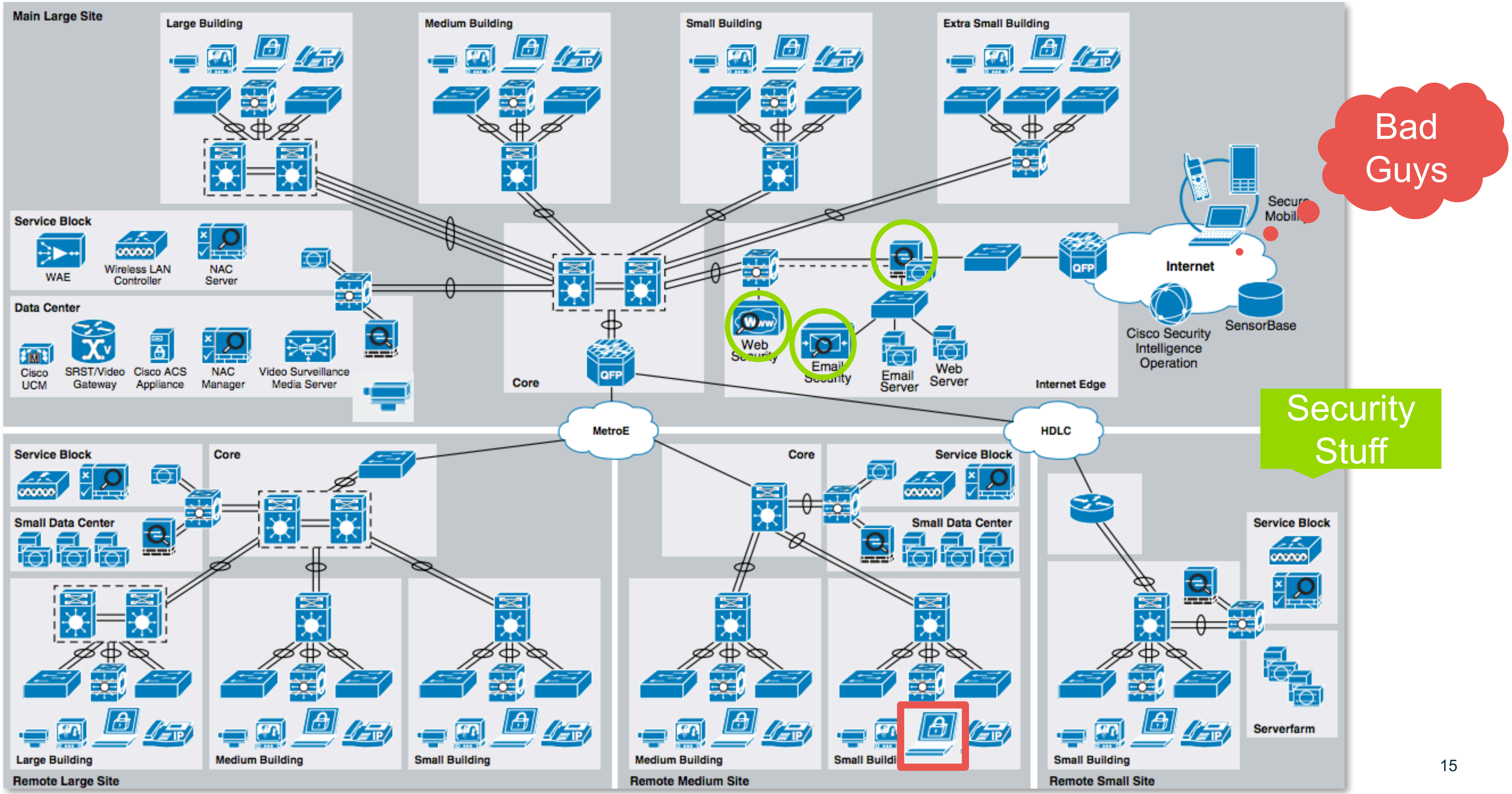
- **The attackers weapon arsenal**

  The attacker can now use the zombies to:

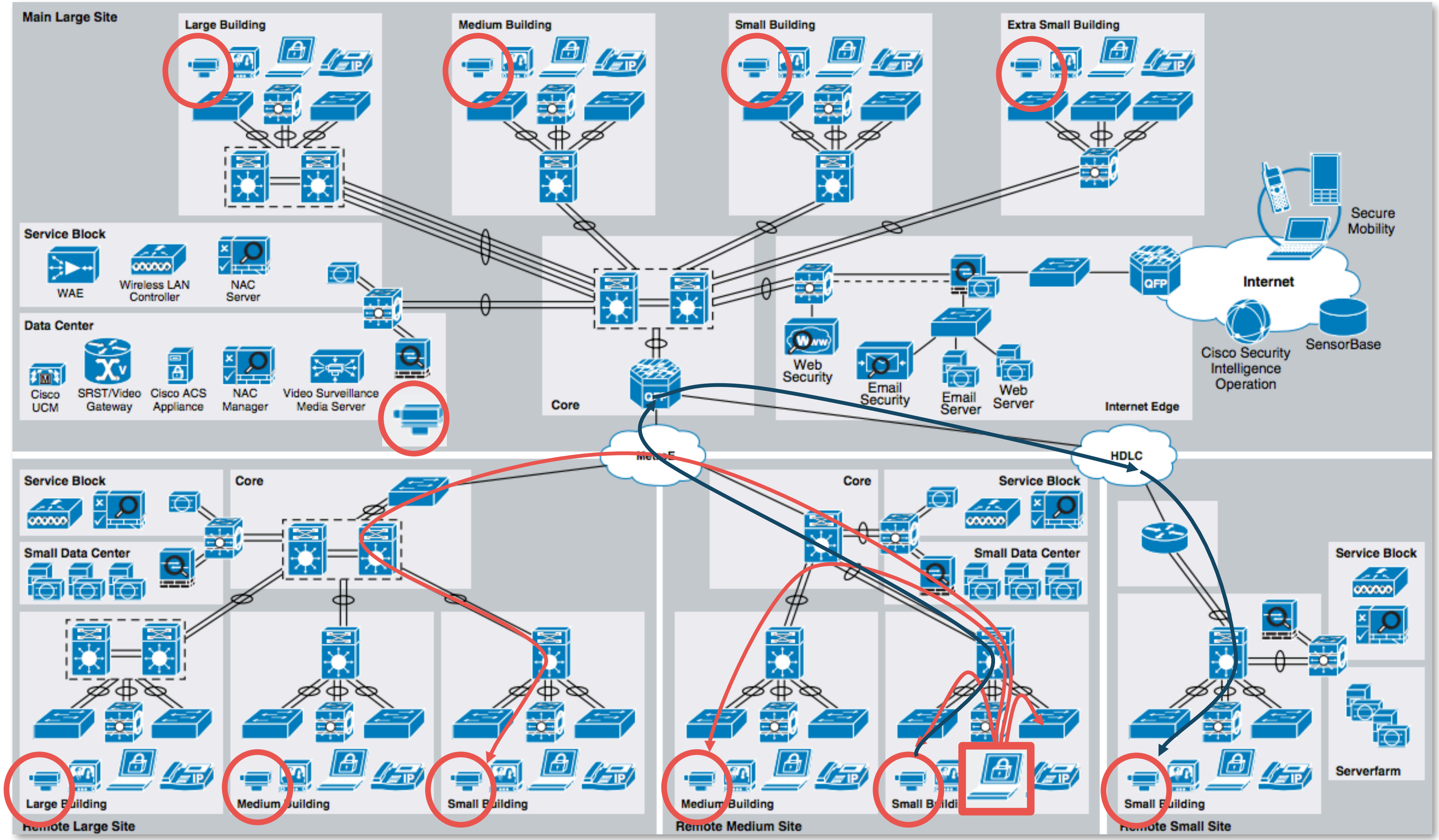
  1. Infect other IoT devices.
  2. Launch outbound attacks against external targets.
  3. Perform reconnaissance on internal networks, followed by targeted attacks against internal targets.

https://hdwallsbox.com/army-undead-fantasy-art-armor-skeletons-artwork-warriors-wallpaper-122347/

A Typical Mid-Enterprise Network



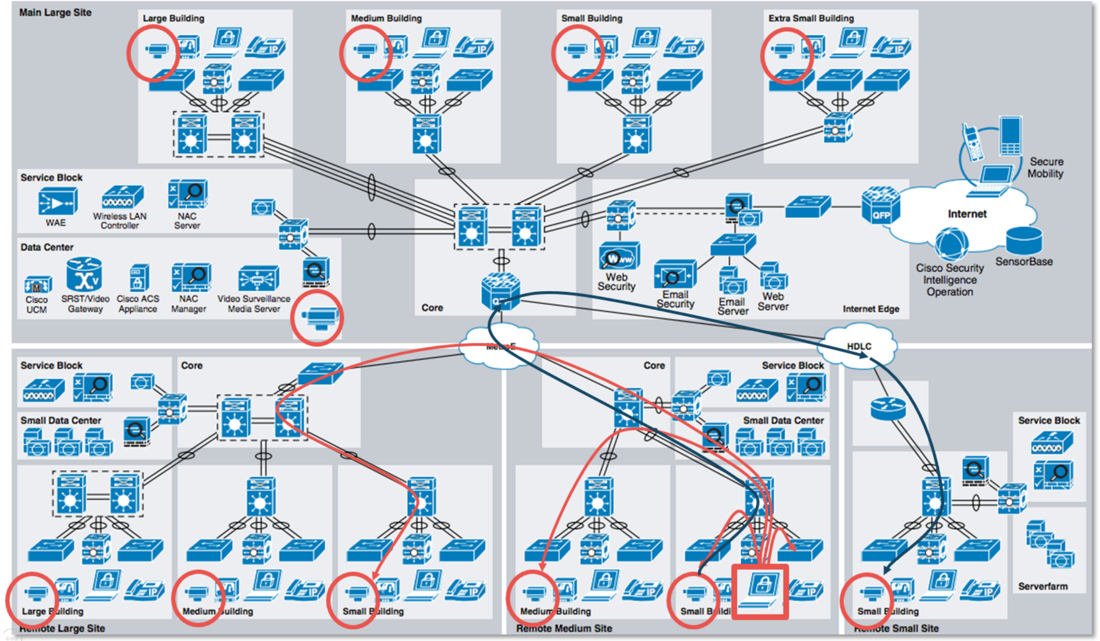
1. Scanning for Devices to Infect



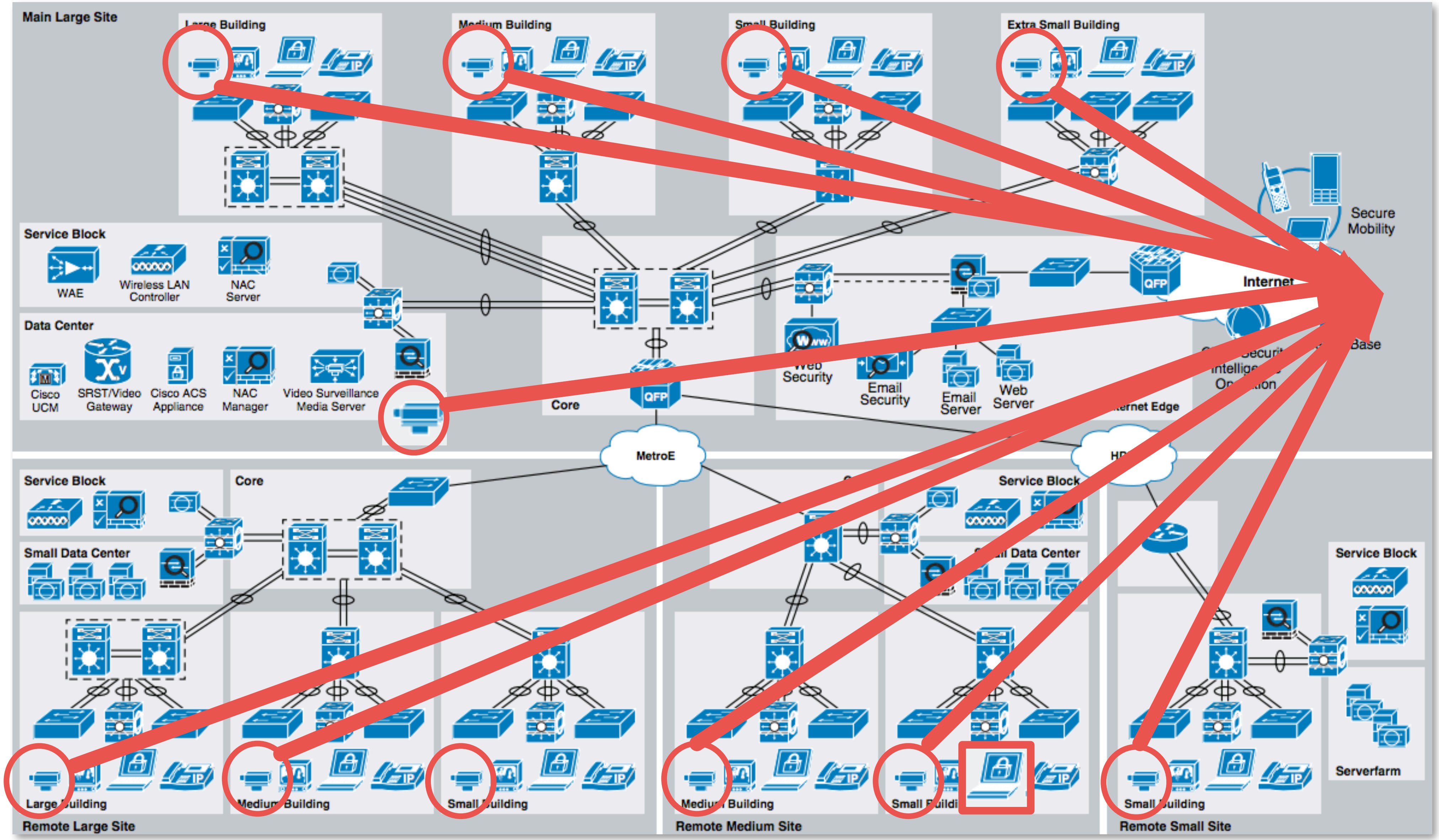
1. Scanning for Devices to Infect

The Scanning activity generates:

- Flood of ARP requests
- Lots of small packets, including TCP SYN’s
- As more devices get infected, the scanning activity will increase, potentially causing serious issues and outages with network devices like firewalls, switches and other stateful devices.
- These kinds of outages have repeatedly happened in the wild, both during the NIMDA, Code Red and Slammer outbreaks in 2001 and also recently during large scale Mirai infections at large European Internet Service Providers.

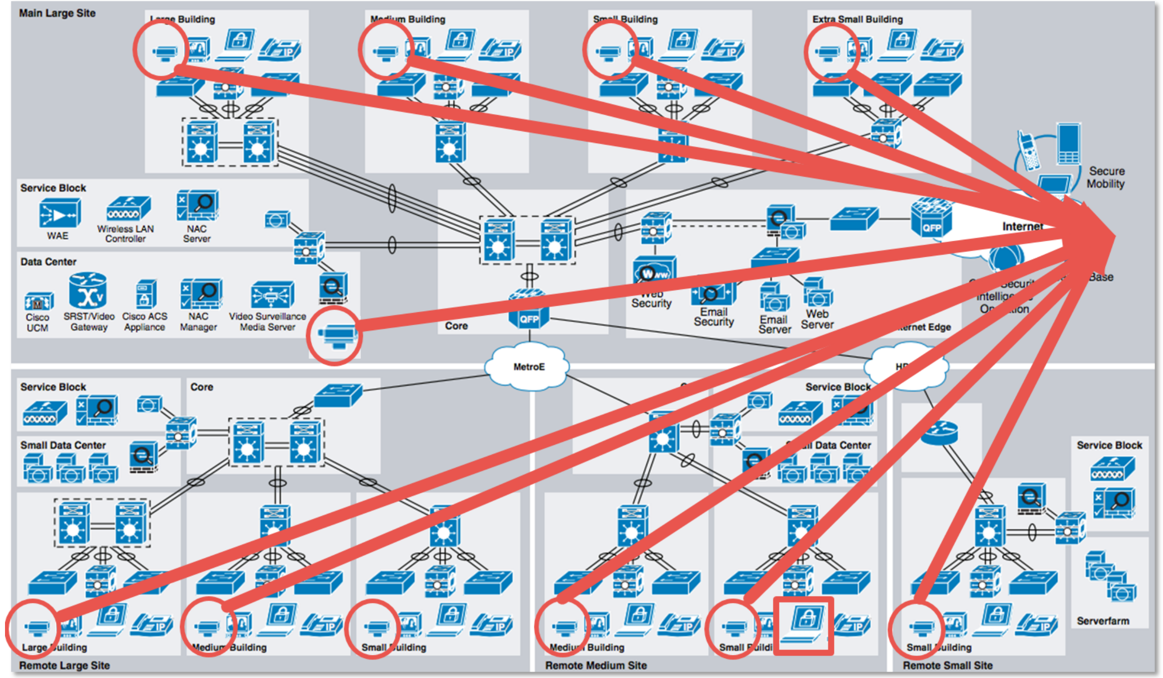


2. Launching Outbound DDoS Attacks



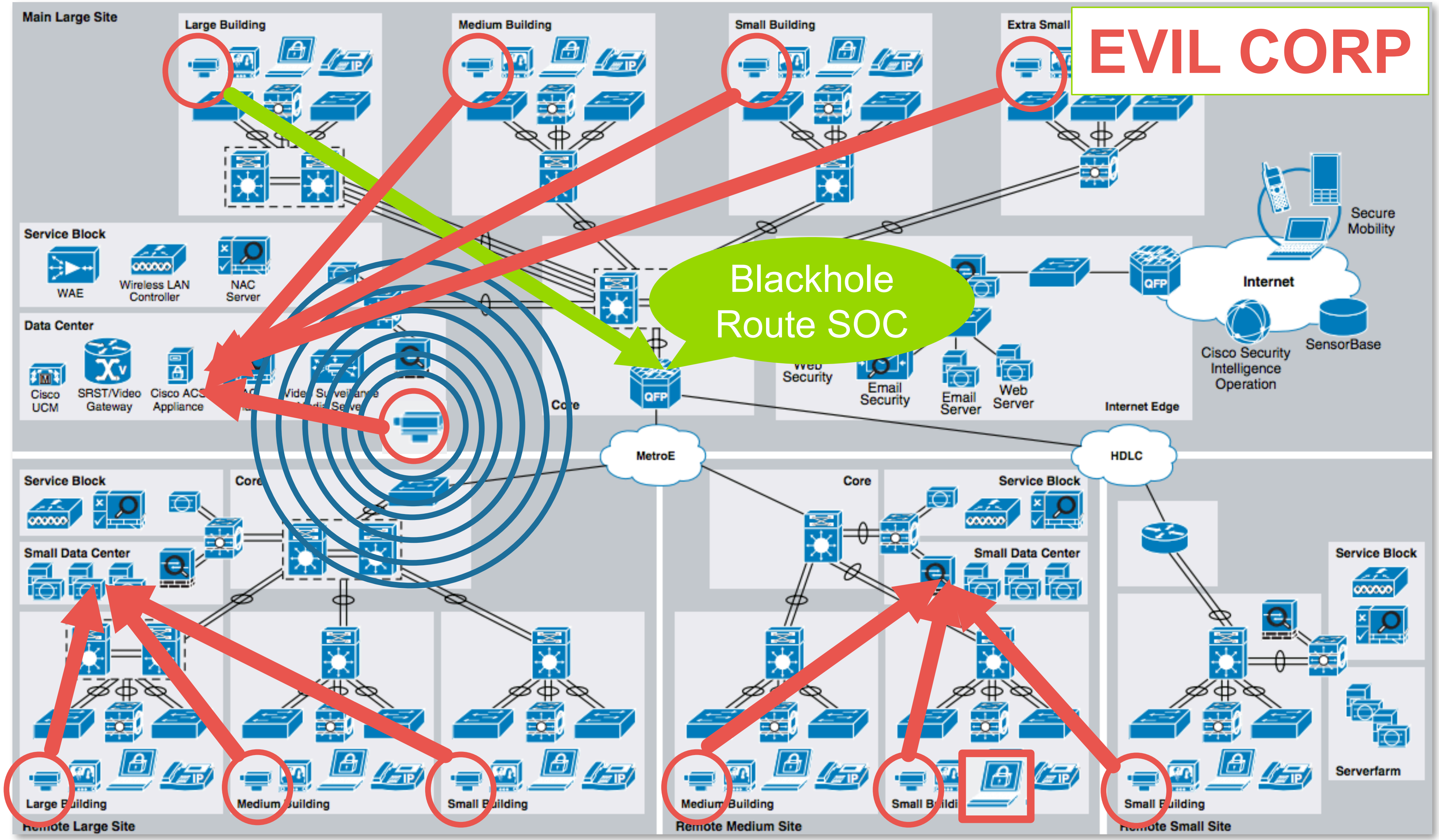
2. Launching Outbound DDoS Attacks

- Attack activity generates a lot of traffic. Mirai can for example launch:
  - UDP/ICMP/TCP packet flooding
  - Reflection attacks using UDP packets with spoofed source IP addresses
  - Application level attacks (HTTP/SIP attacks).
  - Pseudo random DNS label prefix attacks against DNS servers.
- This attack traffic will quickly fill up any internal WAN links and will also will cause havoc with any stateful device on the path, including NGFWs.



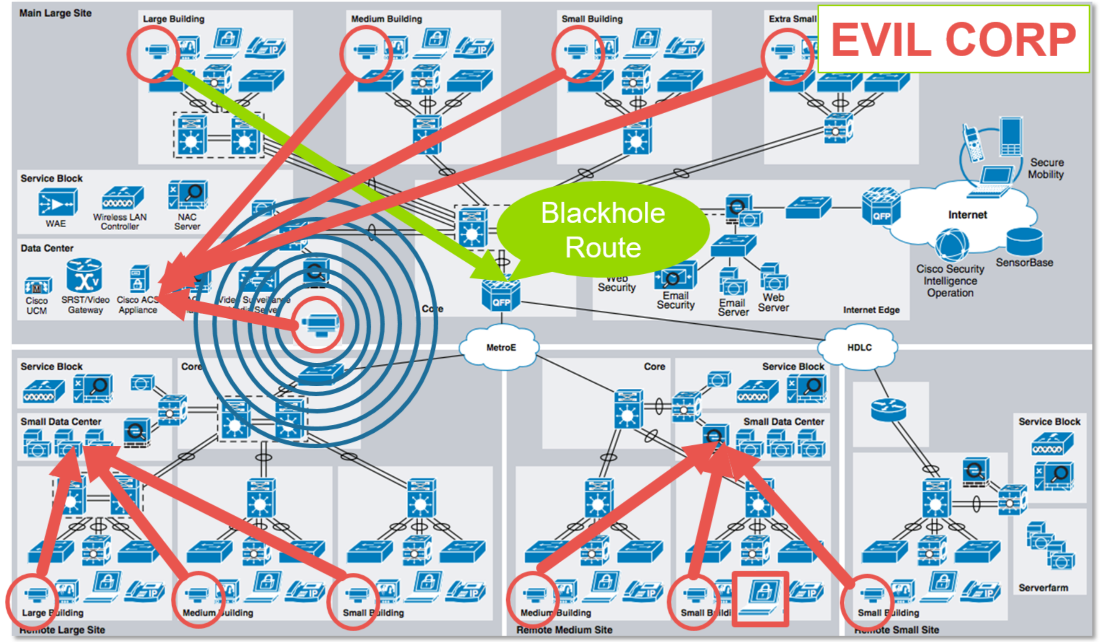
ARBOR NETWORKS

3. Reconnaissance & Internally Facing Attacks



3. Reconnaissance & Internally Facing Attacks

- A clever attacker would scan the internal network to identify vulnerable services and network layout.
- He would then launch attacks against the routing tables to shut out NOC/SOC services, followed by DDoS attacks against internal services.
- This would be devastating as if there are no internal barriers in place, the network would simply collapse.
- After a while, the clever attacker would then stop the attack and send a ransom e-mail, asking for his BTC's…



Defending Against Insider Threats

- Internet Service Providers have successfully been dealing with similar attacks for the last 20 years by following what's called Security Best Current Practices (BCP’s). These basically translate into “**Keep the network up and running**!”
- Service Providers have followed a 6 phase methodology when dealing with attacks:
  - **Preparation**: Prepare and harden the network against attack.
  - **Identification**: Identify that an attack is taking place.
  - **Classification**: Classify the attack.
  - **Traceback**: Where is the attack coming from.
  - **Reaction**: Use the best tool based on the information gathered from the Identification, Classification and Traceback phases to mitigate the attack.
  - **Post-mortem**: Learn from what happened, improve defenses against future attacks.

Defending Against Insider Threats

- These Security Best Practices include:
  - Implementing full Network segmentation and harden (or isolate) vulnerable network devices and services.
  - Developing a DDoS Attack mitigation process.
  - Utilizing flow telemetry to analyze external and internal traffic. This is necessary for attack **detection**, **classification** and **trace back.**
  - Deploying a multi-layered DDoS protection.
  - Scanning for misconfigured and abusable services, this includes NTP, DNS and SSDP service which can be used for amplification attacks.
  - Implementing Anti-Spoofing mechanisms such as Unicast Reverse-Path Forwarding, ACLs, DHCP Snooping & IP Source Guard on all edge devices.

Knowledge & Preparation Are the Keys to Protection

Without the proper knowledge of…

1. DDoS Attack Trends (i.e. Ease, motivations, attack types, relationship with data breach)
2. Best Practices in DDoS Mitigation (i.e. Products, People and Processes)
3. Impact to Your Business (i.e. Downtime, loss revenue, mitigation costs etc.)

…You cannot accurately calculate the risk of a DDoS Attack.

Summary

- **The attackers are now inside the house!**

  The Windows spreader has opened up the possibility to infect internal IoT devices and use them against you.

- **Internal network defenses and security architectures need to be adapted to meet this new threat.**

  Stateful devices will collapse both due to persistent scanning active and also when DDoS attacks are launched.

- **Implementing Security BCP's will help**

  Using Security BCP's will reduce the impact of internal DDoS, in addition this will help to help to secure networks against other security threats as well.

The Walking Dead, Season 6

Zombie Horde by Joakim Olofsson

Q&A / Thank You

For more info, please contact:

CF Chui
Principal Security Technologist
cfchui@arbor.net

ARBOR®
NETWORKS
The Security Division of NETSCOUT

NETSCOUT®

Guardians of the Connected World