# Embedded Systems Hacking and My Plot To Take Over The World

## Version 2.0

What are we going to do tonight, Brain?
the same thing we do every night, Pinky....
...TRY AND TAKE OVER THE WORLD!

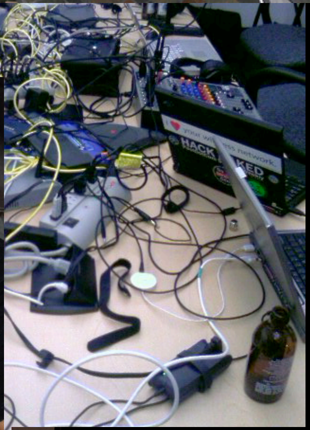
Paul Asadoorian
Founder & CEO, PaulDotCom Enterprises
http://pauldotcom.com
paul@pauldotcom.com

# Who am I?

- I had this really boring slide about who I am
- Then I realized that’s not really who I am
- What follows is the “Powerpoint” version of “a little about me”...

PaulDotCom Security Weekly
http://www.pauldotcom.com

# Podcast



- 2005 - Present
- ~ 200 episodes
- Awards, blah
- Thursdays 7PM EST

# Hack Naked

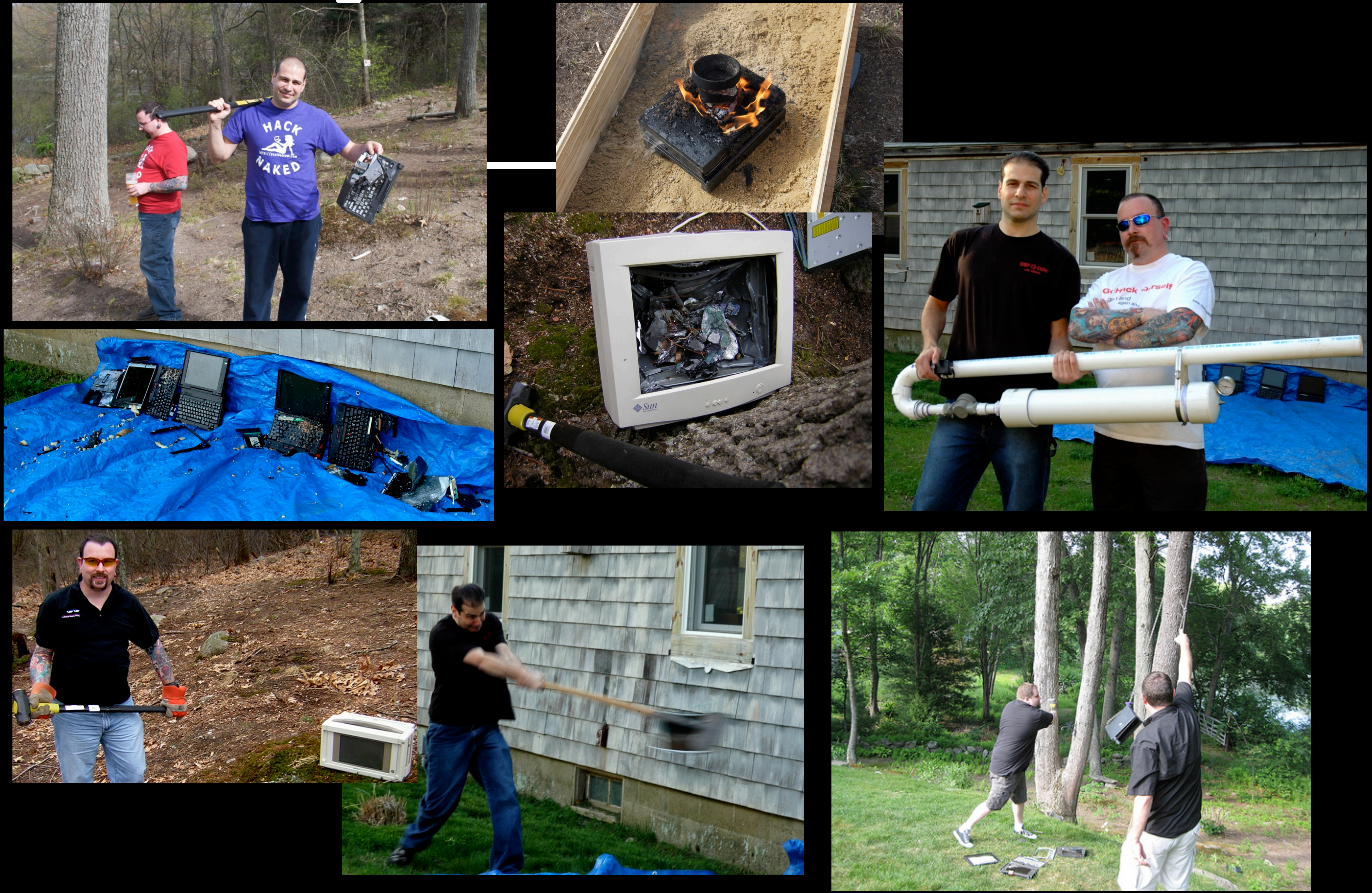
HACK
NAKED
http://pauldotcom.com

## Why Hack Naked?

# Beer

[redacted]

# Computer Destruction



# PaulDotCom

John "Father John" Strand

Paul "Salad Shooter" Asadoorian

Larry "Dirty Uncle" Pesce

Mick "Jr. Salad Shooter" Douglas

?

"Byte_Bucket"

Carlos "Dark0perator" Perez

Mike "The Original Intern" Perez

Mark Baggett

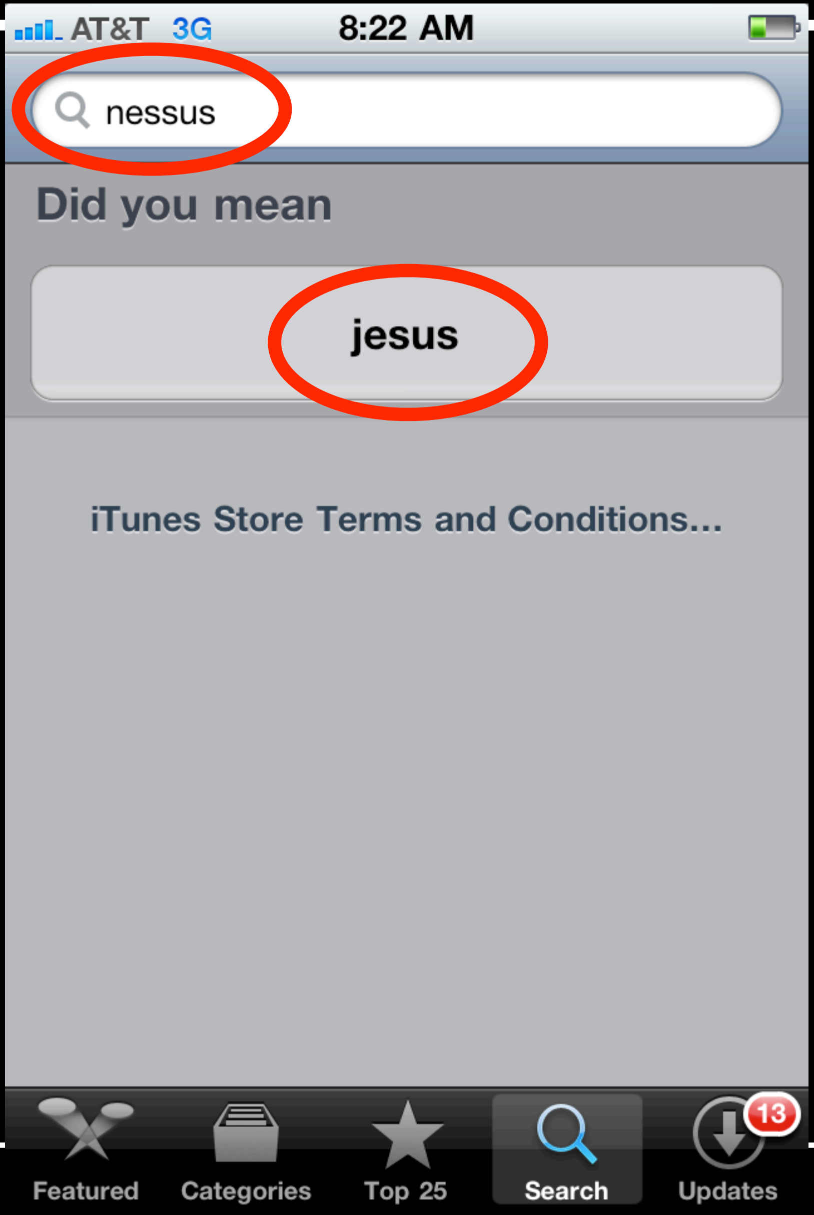
Darren "Girly Mustache" Wigley

# “Hail Nessus!”

- My day job: I work for Tenable Network Security as a “Product Evangelist”
- I use Tenable products and write blogs, publish podcasts, teach courses, and produce videos
- http://blog.tenablesecurity.com

# Recently we released an iPhone app

Looking for Nessus?



AT&T 3G 8:22 AM

nessus

Did you mean

jesus

iTunes Store Terms and Conditions...

Find Jesus?

# Taking Over The World

- Many have tried
- No one truly successful
- What are the three things you need to take over the world?
  - Yes, I’ve spent time thinking about this
- All geeks ~~like~~ deal with “specifications” and “Requirements”

# Requirements For World Domination

1. **Money** - You need to buy stuff, like armies, countries, pay people off, etc...

2. **Power** - You need the ability to use those resources to influence & control people

3. **Stealth** - If everyone knows about your plan, it is doomed from the beginning

# Using Embedded Systems To Make Money

- **Video games** - Most are involved in commerce and network connected
- **Entertainment** - Apple TV/iTV, Roku, all link back to your credit card somehow
- **Wireless routers** - Route your traffic when doing online banking, Paypal, Ebay, etc...
- **Printers/Fax** - How many times have you printed sensitive information?

# Using Embedded Systems To Gain Power

- Network traffic (e.g. information) flows through them
- Information = Power
  - The ability to manipulate information is powerful
- Multiple computers can be controlled at once

# Using Embedded Systems To Gain Power

- Embedded systems are an integral to controlling water, electricity, and sewage treatment

- See research from Josh Wright (http://www.willhackforsushi.com) and Travis Goodspeed (http://travisgoodspeed.blogspot.com/)

- "Advanced Metering Infrastructure Attack Methodology" from Inguardians

# Benefits To Targeting Embedded Systems - Stealth

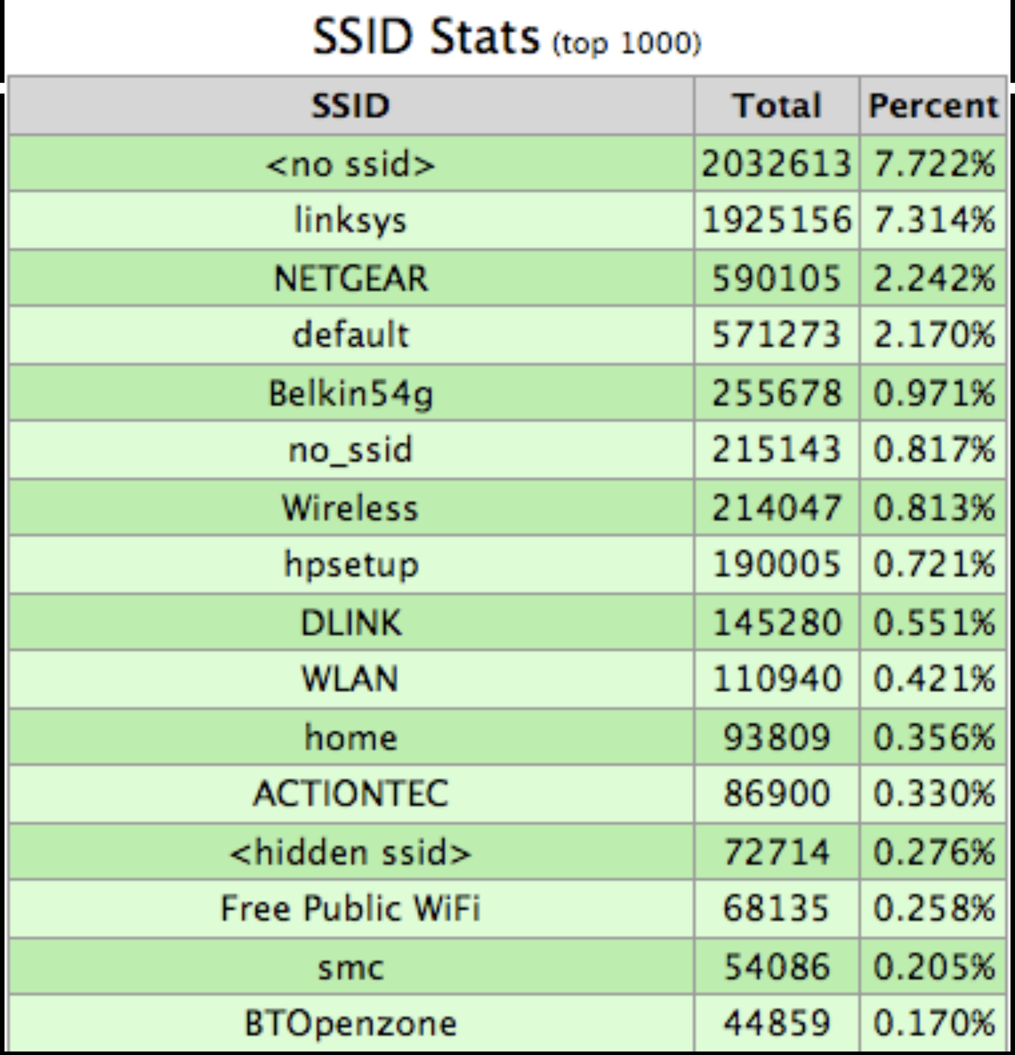
- No one pays attention to them until they are broken

- Security is left out to save resources, make it easy, and money (as is logging)
  - Vendors are focused on profit, which also never equals security
  - Competition has driven vendors to cut costs to make products cheaper
- Potentially no interactive user (mouse/keyboard)

# Benefits Of Targeting Embedded Systems - Stealth

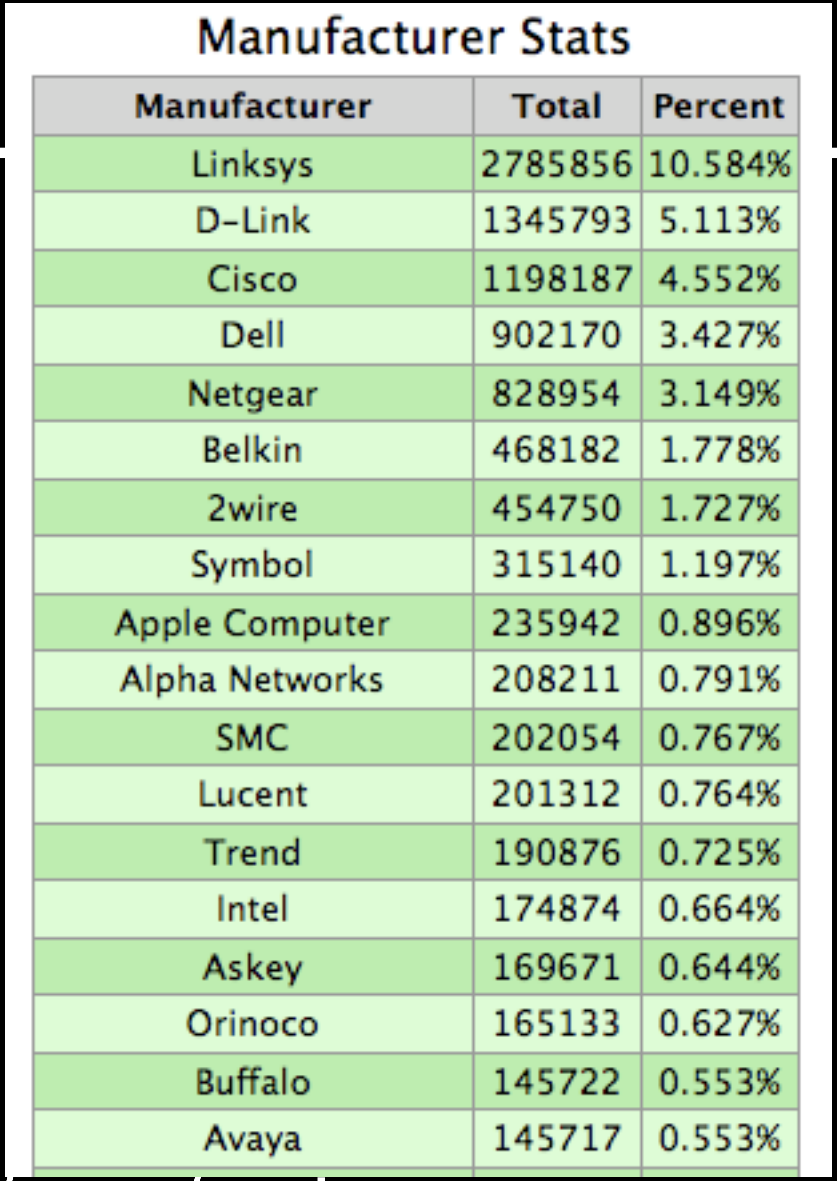
- Embedded systems contain vulnerabilities that go unnoticed because everyone looking for them does not have every device that was ever made
- Thats not to say you **can't** get them or scan the Internet to find them
- "Can you send me a free router in exchange for some security testing?"

# They Are Everywhere



SSID Stats (top 1000)

| SSID | Total | Percent |
|---|---|---|
| <no ssid> | 2032613 | 7.722% |
| linksys | 1925156 | 7.314% |
| NETGEAR | 590105 | 2.242% |
| default | 571273 | 2.170% |
| Belkin54g | 255678 | 0.971% |
| no_ssid | 215143 | 0.817% |
| Wireless | 214047 | 0.813% |
| hpsetup | 190005 | 0.721% |
| DLINK | 145280 | 0.551% |
| WLAN | 110940 | 0.421% |
| home | 93809 | 0.356% |
| ACTIONTEC | 86900 | 0.330% |
| <hidden ssid> | 72714 | 0.276% |
| Free Public WiFi | 68135 | 0.258% |
| smc | 54086 | 0.205% |
| BTOpenzone | 44859 | 0.170% |

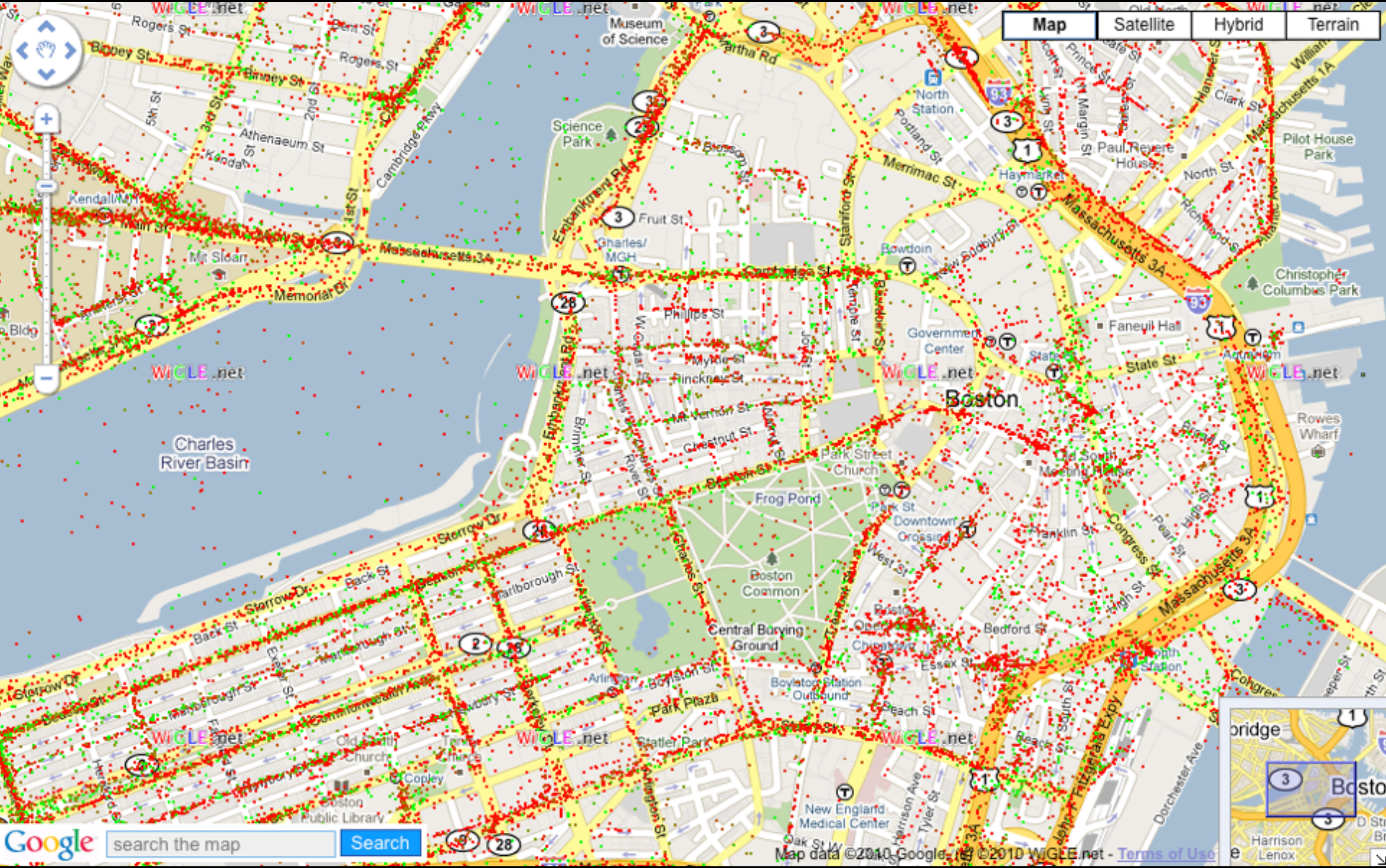


Manufacturer Stats

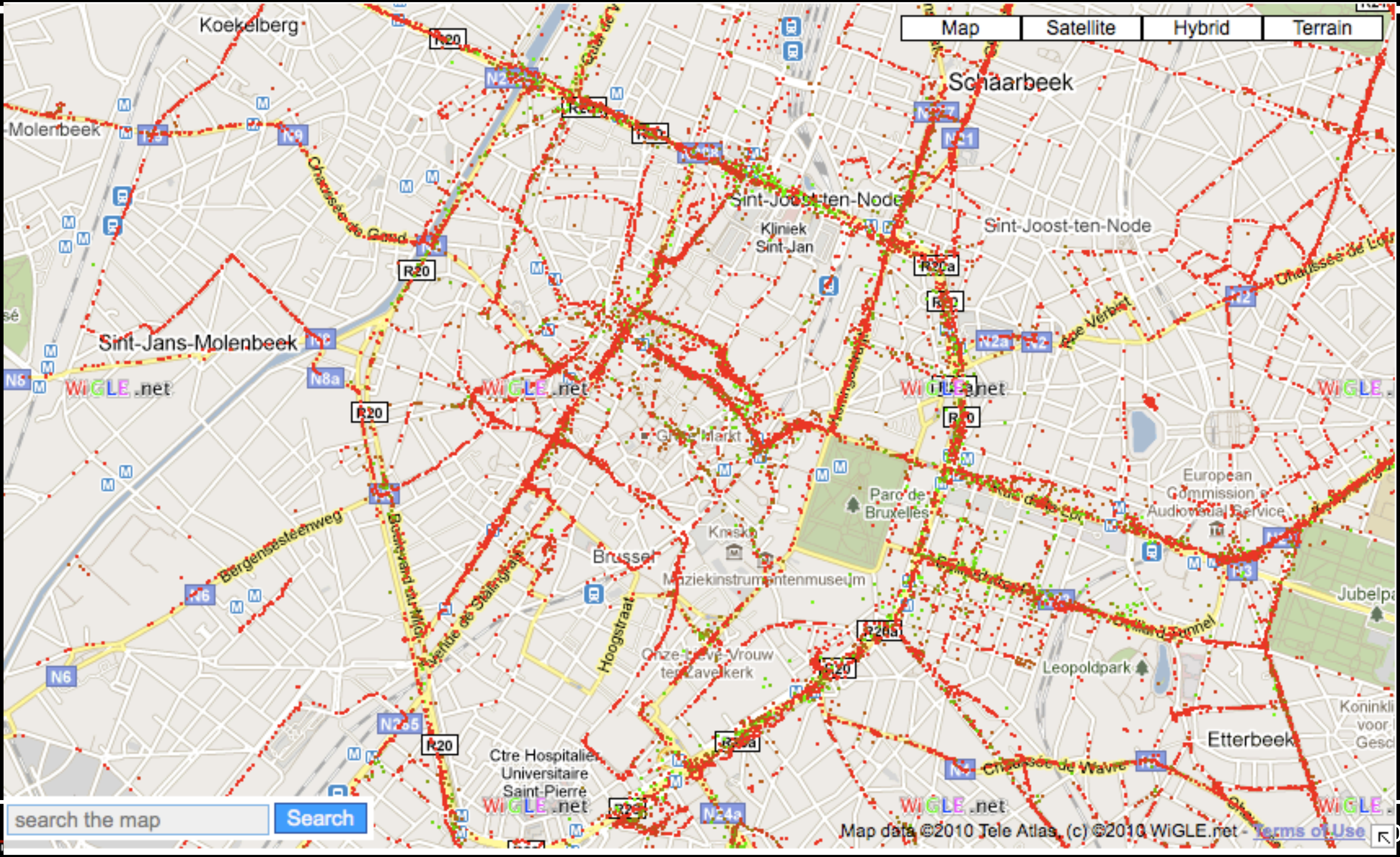
| Manufacturer | Total | Percent |
|---|---|---|
| Linksys | 2785856 | 10.584% |
| D-Link | 1345793 | 5.113% |
| Cisco | 1198187 | 4.552% |
| Dell | 902170 | 3.427% |
| Netgear | 828954 | 3.149% |
| Belkin | 468182 | 1.778% |
| 2wire | 454750 | 1.727% |
| Symbol | 315140 | 1.197% |
| Apple Computer | 235942 | 0.896% |
| Alpha Networks | 208211 | 0.791% |
| SMC | 202054 | 0.767% |
| Lucent | 201312 | 0.764% |
| Trend | 190876 | 0.725% |
| Intel | 174874 | 0.664% |
| Askey | 169671 | 0.644% |
| Orinoco | 165133 | 0.627% |
| Buffalo | 145722 | 0.553% |
| Avaya | 145717 | 0.553% |

http://wigle.net/gps/gps/main/ssidstats

# In Places Like Boston



# Or Maybe Brussels...



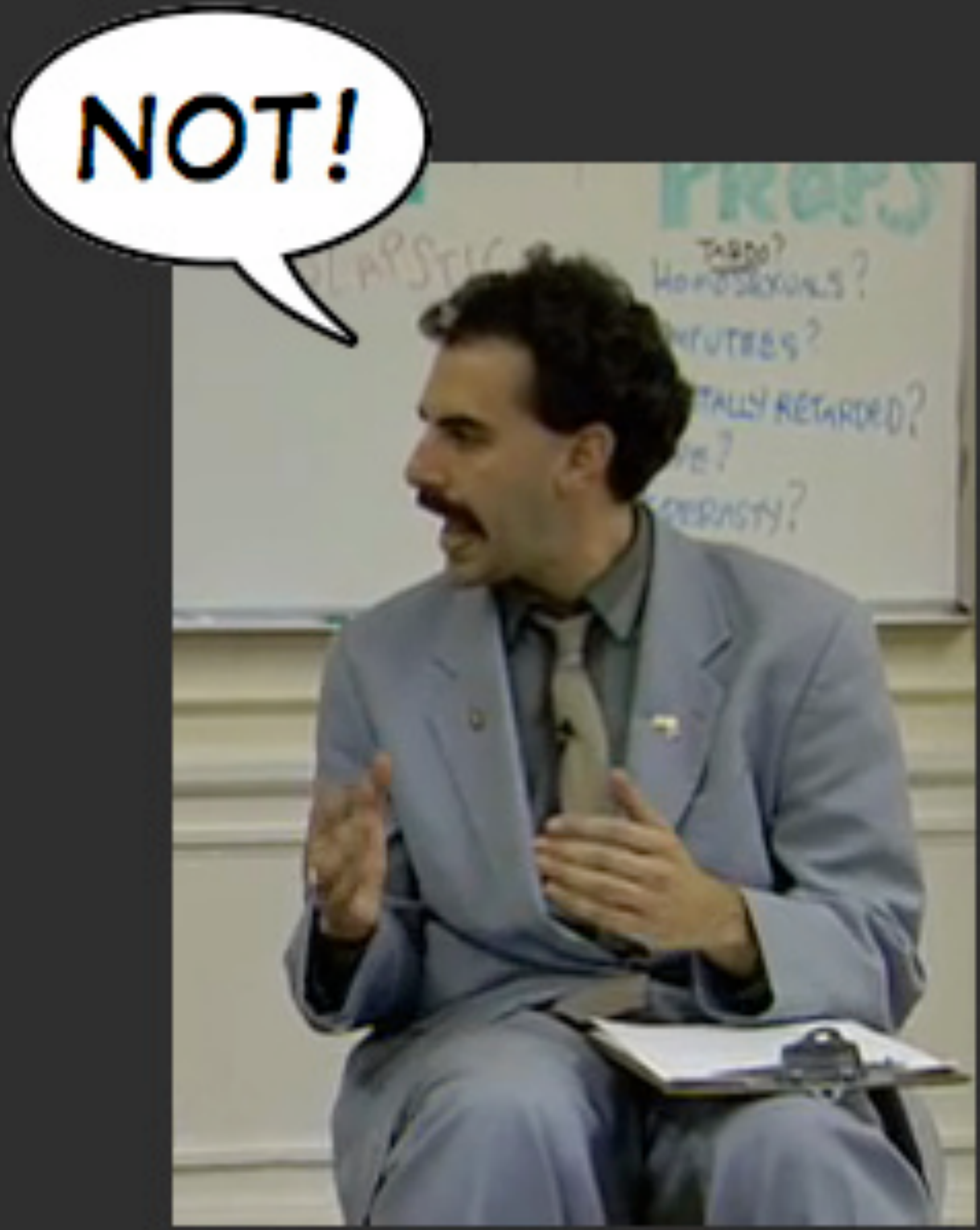
Map data ©2010 Tele Atlas, (c) ©2010 WiGLE.net - Terms of Use

# And They Are Vulnerable...

*Researchers scanning the internet for vulnerable embedded devices have found nearly 21,000 routers, webcams and VoIP products open to remote attack. Their administrative interfaces are viewable from anywhere on the internet and their owners have failed to change the manufacturer's default password.*

*http://www.wired.com/threatlevel/2009/10/vulnerable-devices/#ixzz0foWysVrp*

*“The researchers have provided ISPs with their findings in the hope that they will do something to protect vulnerable customers.”*


NOT!
PROPS
TABOO?
HOMOSEXUALS?
TALLY RETARDED?

# And No One Wants To Be Responsible For Them

*Chen said he contacted Time Warner's security department four weeks ago and was told that the company was aware of the security vulnerability but **"cannot do anything about it."***

*Time Warner's Dudley says the SMC8014 modem/routers are just a small portion of the **14 million devices** its customers are using.*

http://www.wired.com/threatlevel/2009/10/time-warner-cable/

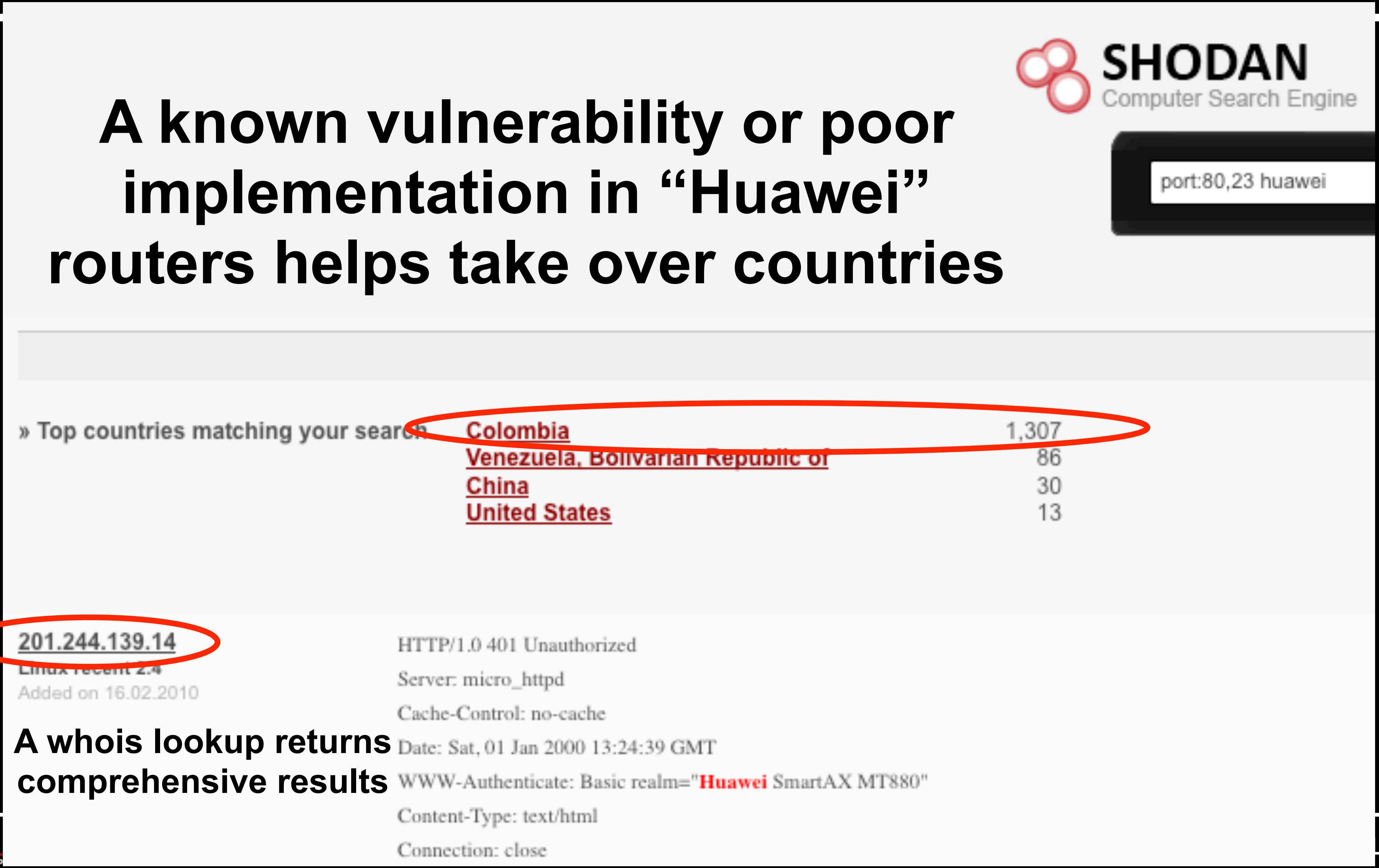
# What if “Bob” Scanned the Internet?

- Use Google, find most popular ISPs that provide cable modem routers to users (or other interesting devices)
- Use ARIN to discover the IP address ranges assigned to those ISPs
- Use Nmap to discover all devices that have port 80 open and identify the service/banner
- Manually poke through results and see what you find
  - Or automate something to find vulnerabilities, exploit them, and upload custom configurations and/or firmware

# Example Vulnerabilities We Could Look For

- Wireless Routers - TONS of FAIL on the Internet
  - Default, weak, or missing passwords are COMMON
  - Linksys HNAP - Information leakage and lame denial of service with no mitigation
- Printers - JetDirect authentication weaknesses, HP Multifunctions, Lanier printer information disclosure
- Roku Player - Entertainment device

# Shodan is Handy For Exploring The Inernet



A known vulnerability or poor implementation in “Huawei” routers helps take over countries

SHODAN

Computer Search Engine

port:80,23 huawei

» Top countries matching your search

| | |
|---|---|
| Colombia | 1,307 |
| Venezuela, Bolivarian Republic of | 86 |
| China | 30 |
| United States | 13 |

201.244.139.14

Linux recent 2.4

Added on 16.02.2010

```
HTTP/1.0 401 Unauthorized
Server: micro_httpd
Cache-Control: no-cache
Date: Sat, 01 Jan 2000 13:24:39 GMT
WWW-Authenticate: Basic realm="Huawei SmartAX MT880"
Content-Type: text/html
Connection: close
```

A whois lookup returns comprehensive results

# Scanning the Internet is Time Consuming

- Scanning the Internet is fun (so Bob tells me)
- It takes a long time, even when limiting to one port

```
# nmap --version-light --open --min-hostgroup 1024 -T4 -n
    -PN -oG results.gnmap -sV -p 80 -iL isp.targetips
```

**524288 IP addresses (32620 hosts up) scanned in 9769.46 seconds (2.7 hours)**

**2272512 IP addresses (2272512 hosts up) scanned in 135156.66 seconds (37.5 Hours)**

# Finding Devices Without Scanning The Internet

- NTP could be used to identify devices
  - Example: http://carnal0wnage.blogspot.com/2010/04/network-time-protocol-ntp-fun.html
- DNS zone transfers from certain places reveal interesting results
- Brute-forcing DNS sub-domains can reveal hosts too
  - Example: http://www.gnucitizen.org/blog/hacking-linksys-ip-cameras-pt-6/

# NTP: All your ntp are point to us

- Netgear shipped thousands of routers in 2003 and pointed them to ntp1.cs.wisc.edu
  - http://pages.cs.wisc.edu/~plonka/netgear-sntp/
- Issued firmware fix, but who does that?
- Routers still point to it, and thanks to HD Moore we can query it easily with metasploit
- Gives us a list of Netgear routers that Bob would attack

# Metasploit NTP Module

```
msf > use auxiliary/scanner/ntp/ntp_monlist
msf auxiliary(ntp_monlist) > set RHOSTS ntp1.cs.wisc.edu
RHOSTS => ntp1.cs.wisc.edu
msf auxiliary(ntp_monlist) > run

[*] Sending probes to 128.105.39.11->128.105.39.11 (1 hosts)
[*] 128.105.39.11:123 205.237.147.11:23457 (128.105.39.11)
[*] 128.105.39.11:123 86.29.31.176:23457 (128.105.39.11)
[*] 128.105.39.11:123 209.192.117.17:23457 (128.105.39.11)
[*] 128.105.39.11:123 70.54.203.193:60128 (128.105.39.11)
[*] 128.105.39.11:123 222.254.78.74:10001 (128.105.39.11)
```

Lots of DSL/Cable Providers on the list

**What are chances these users have not updated firmware?**

```
71.161.67.98 domain name pointer adsl-67-161-71.shv.bellsouth.net.
76.72.108.68 domain name pointer ip68-108-72-76.lv.lv.cox.net.
117.131.29.65 domain name pointer CPE-65-29-131-117.wi.res.rr.com
45.21.110.76 domain name pointer c-76-110-21-45.hsd1.fl.comcast.net
61.195.100.98 domain name pointer rrcs-98-100-195-61.central.biz.rr.com.
164.133.254.76 domain name pointer adsl-76-254-133-164.dsl.skt2ca.sbcglobal.net.
```

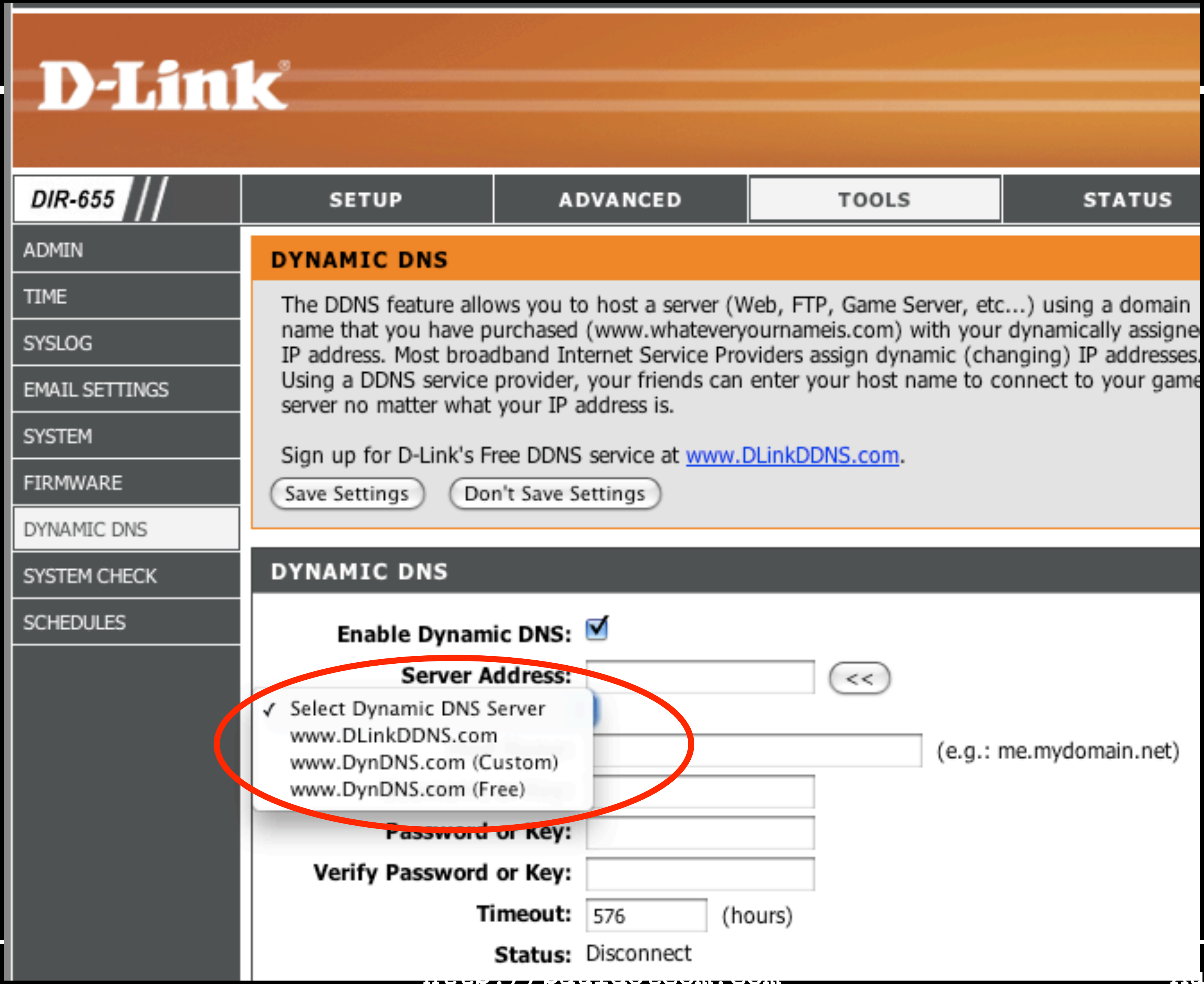
# DNS Zone Transfer - MUCH faster!

```
# time host -la ourlinksys.com 66.161.11.121 >
ourlinksys.com.out

real 0m2.564s
user 0m0.456s
sys  0m0.068s

# wc -l ourlinksys.com.out 120815 ourlinksys.com.out
```

This no longer works with the above domain since I accidentally published the information without sanitizing.

Check out Metasploit's "gather/dns_enum" module written by Carlos Perez

# Target specific devices



**DYNAMIC DNS**

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigne IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com.

**DYNAMIC DNS**

Enable Dynamic DNS: ☑

Server Address:

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

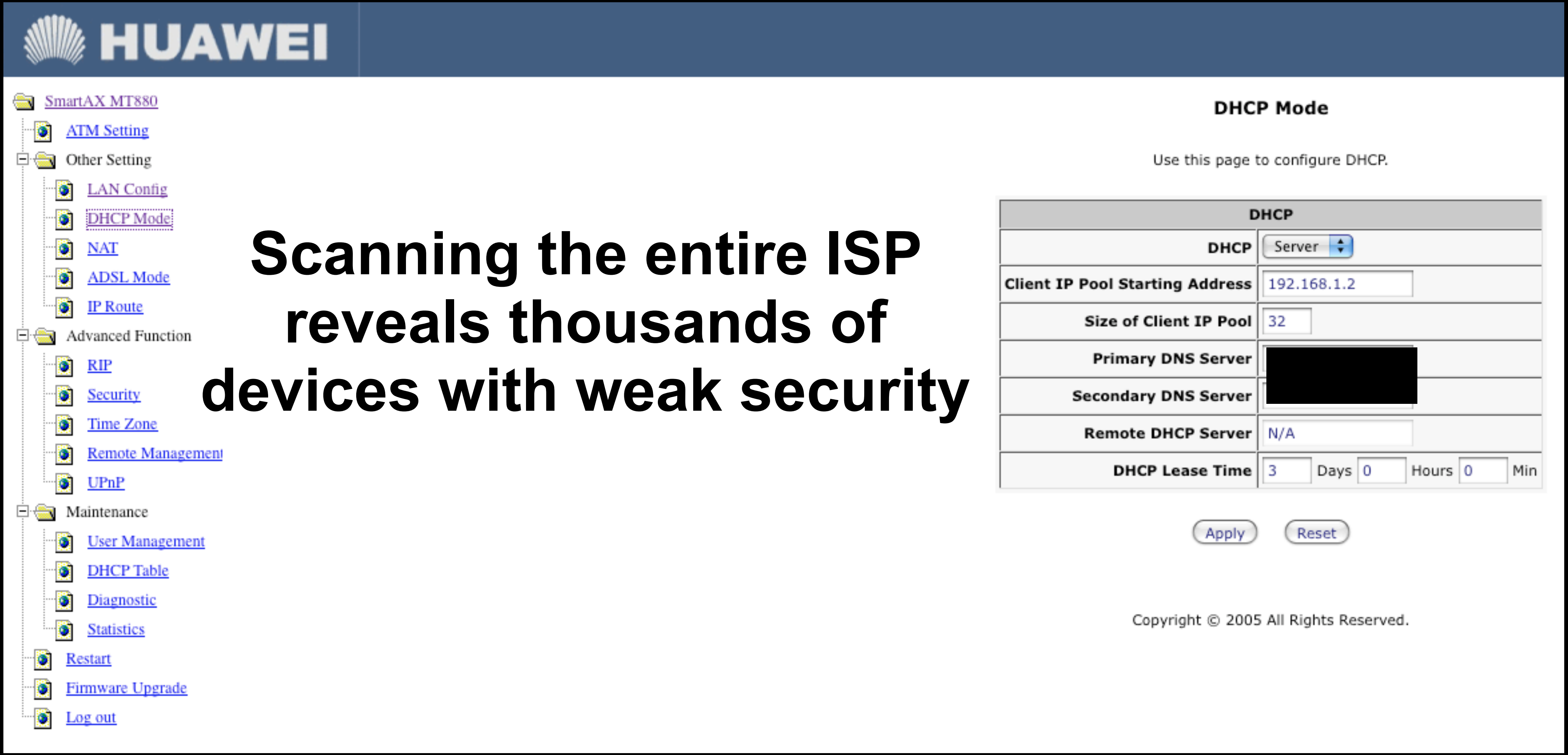
Password or Key:

Verify Password or Key:

Timeout: 576 (hours)

Status: Disconnect

# Now that you've found them..



**Scanning the entire ISP reveals thousands of devices with weak security**

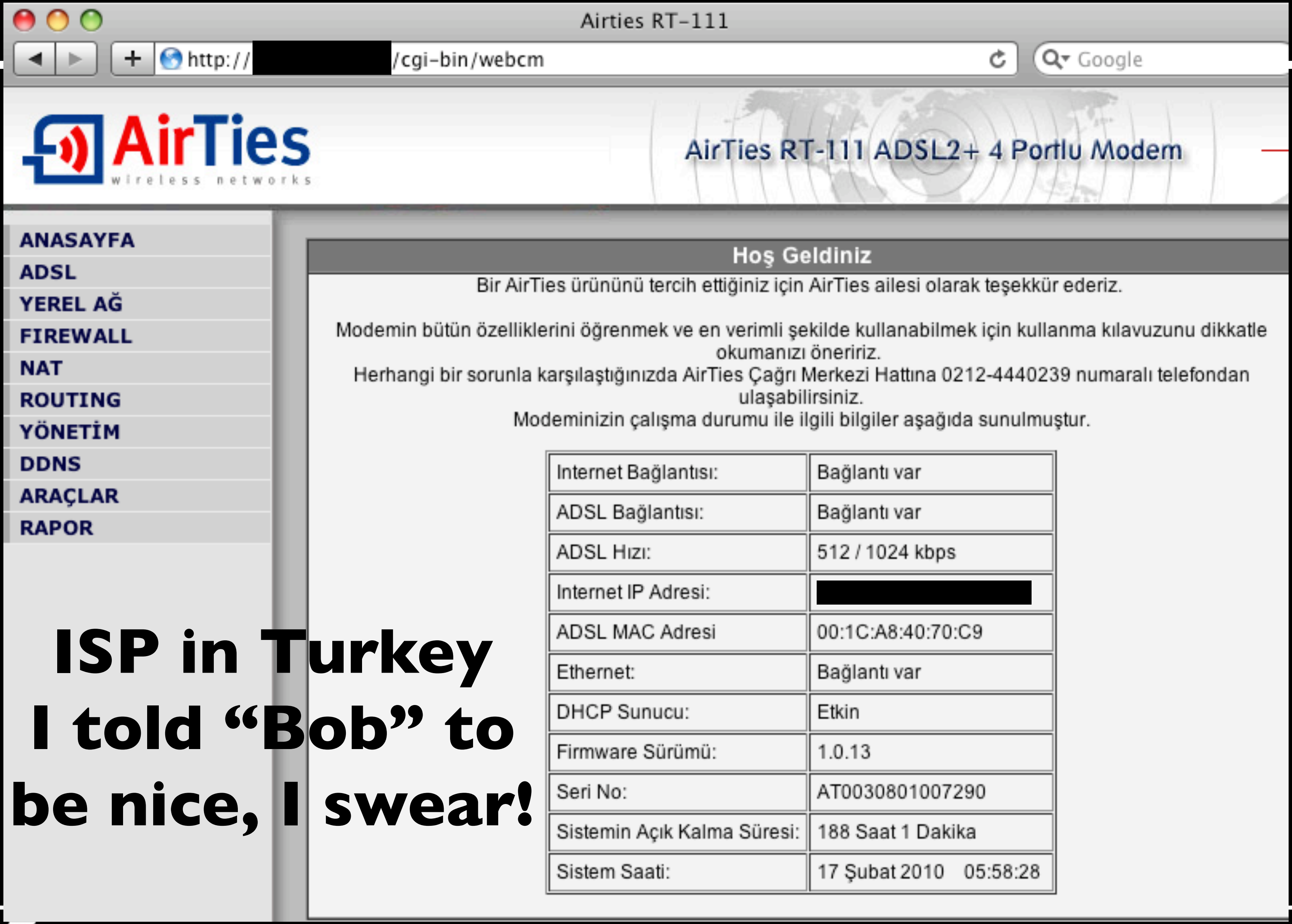
### DHCP Mode

Use this page to configure DHCP.

| DHCP | |
|---|---|
| DHCP | Server |
| Client IP Pool Starting Address | 192.168.1.2 |
| Size of Client IP Pool | 32 |
| Primary DNS Server | [redacted] |
| Secondary DNS Server | [redacted] |
| Remote DHCP Server | N/A |
| DHCP Lease Time | 3 Days 0 Hours 0 Min |

Copyright © 2005 All Rights Reserved.

# This Required NO PASSWORD


Airties RT-111
http://[redacted]/cgi-bin/webcm
Google
AirTies wireless networks
AirTies RT-111 ADSL2+ 4 Portlu Modem
ANASAYFA
ADSL
YEREL AĞ
FIREWALL
NAT
ROUTING
YÖNETİM
DDNS
ARAÇLAR
RAPOR

**Hoş Geldiniz**

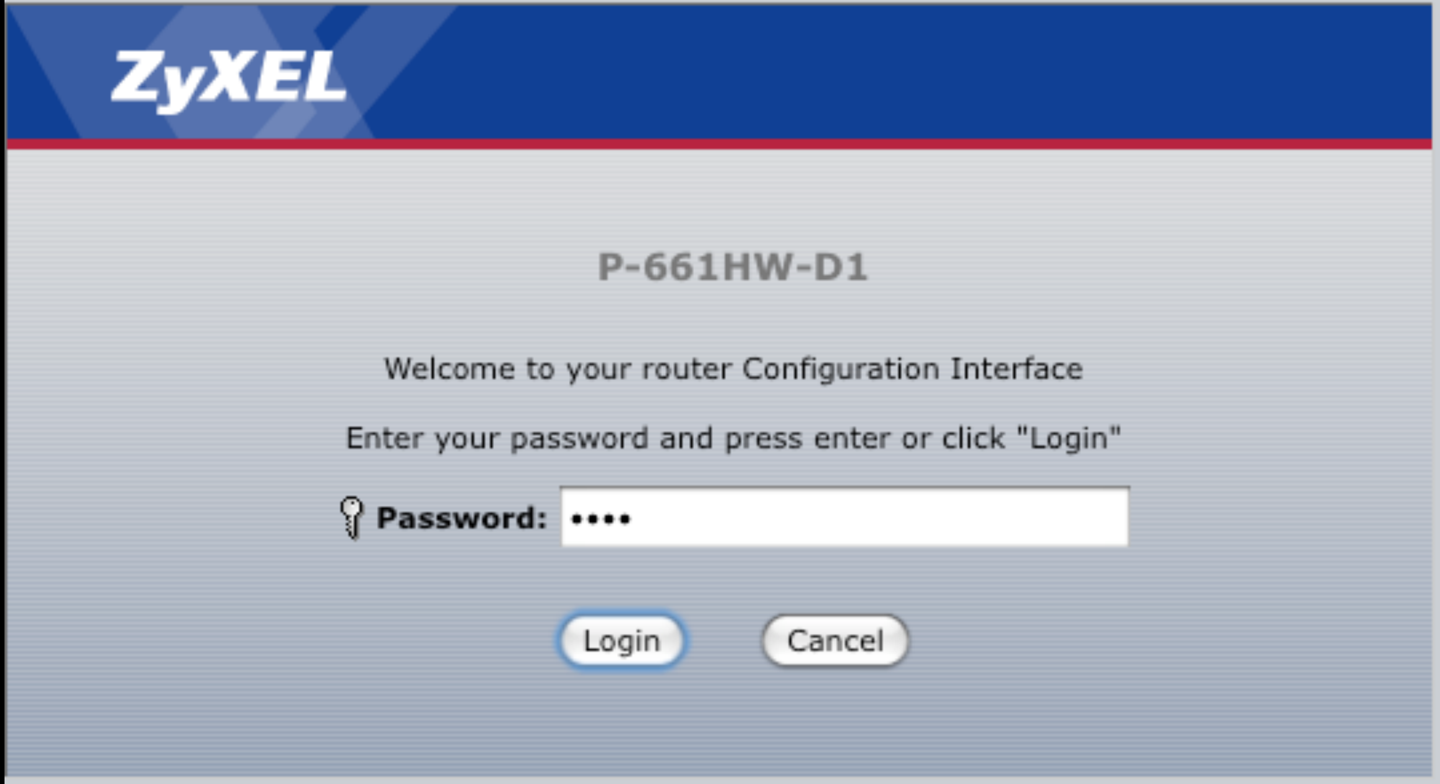
Bir AirTies ürününü tercih ettiğiniz için AirTies ailesi olarak teşekkür ederiz.

Modemin bütün özelliklerini öğrenmek ve en verimli şekilde kullanabilmek için kullanma kılavuzunu dikkatle okumanızı öneririz.
Herhangi bir sorunla karşılaştığınızda AirTies Çağrı Merkezi Hattına 0212-4440239 numaralı telefondan ulaşabilirsiniz.
Modeminizin çalışma durumu ile ilgili bilgiler aşağıda sunulmuştur.

| | |
|---|---|
| Internet Bağlantısı: | Bağlantı var |
| ADSL Bağlantısı: | Bağlantı var |
| ADSL Hızı: | 512 / 1024 kbps |
| Internet IP Adresi: | [redacted] |
| ADSL MAC Adresi | 00:1C:A8:40:70:C9 |
| Ethernet: | Bağlantı var |
| DHCP Sunucu: | Etkin |
| Firmware Sürümü: | 1.0.13 |
| Seri No: | AT0030801007290 |
| Sistemin Açık Kalma Süresi: | 188 Saat 1 Dakika |
| Sistem Saati: | 17 Şubat 2010 05:58:28 |

**ISP in Turkey**
**I told "Bob" to be nice, I swear!**

# The Password Is Already There!



P-661HW-D1

Welcome to your router Configuration Interface

Enter your password and press enter or click "Login"

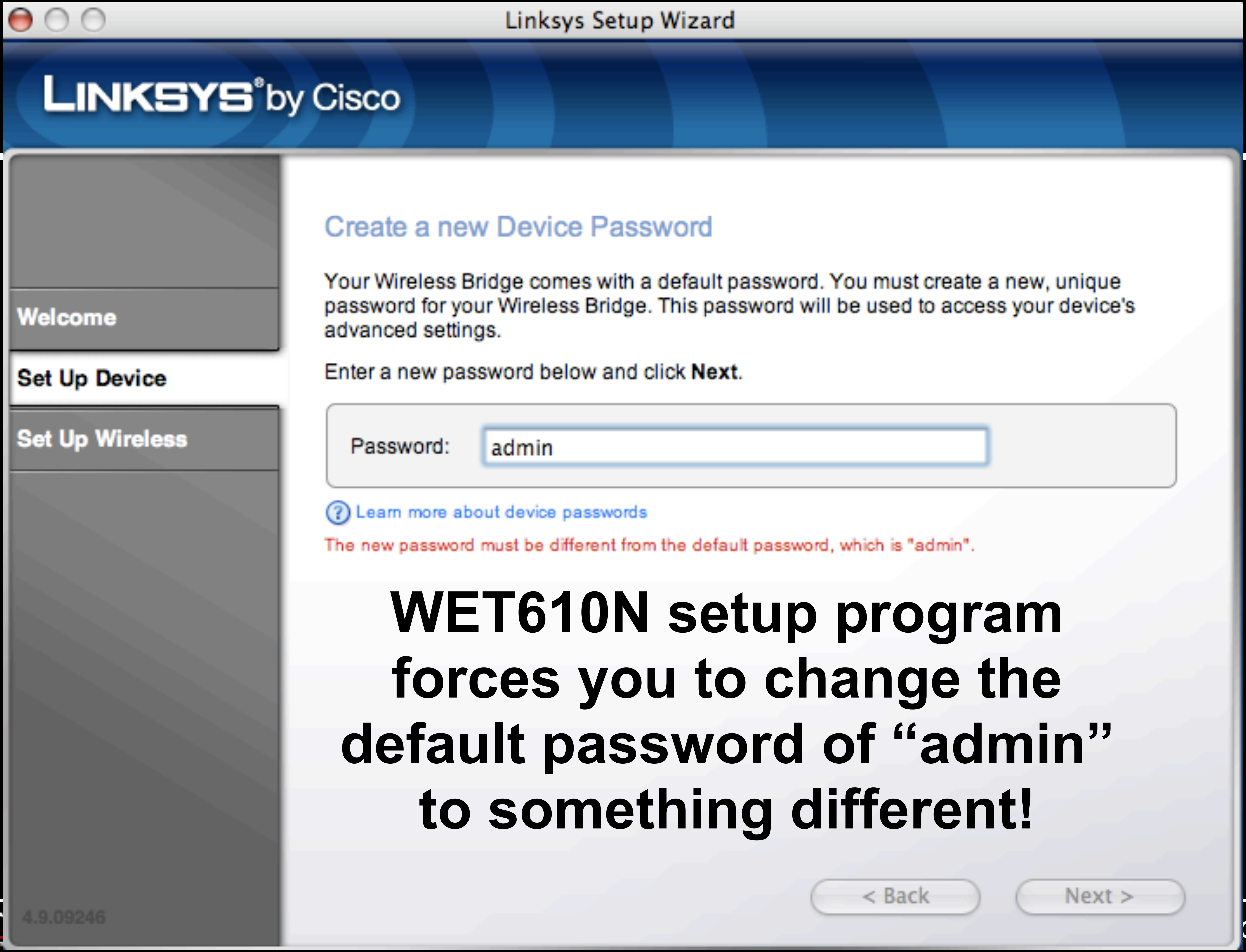
Password: ••••

# This Gets Scary

- A certain ISP based in Turkey left default or blank passwords on seemingly every router
- This helps in our plot for world domination:

1. Target geographic regions, exploit vulnerabilities exposed by that particular ISP+Cable Modem combo
2. Change DNS servers and control user’s “Internets”
3. Change passwords and lock out user and ISP (not too stealthy)
4. More stealthy: Upload new firmware to provide new functionality (like password logging, SSL MiTM, etc...)

# EPIC WIN!



Linksys Setup Wizard

Create a new Device Password

Your Wireless Bridge comes with a default password. You must create a new, unique password for your Wireless Bridge. This password will be used to access your device's advanced settings.

Enter a new password below and click **Next**.

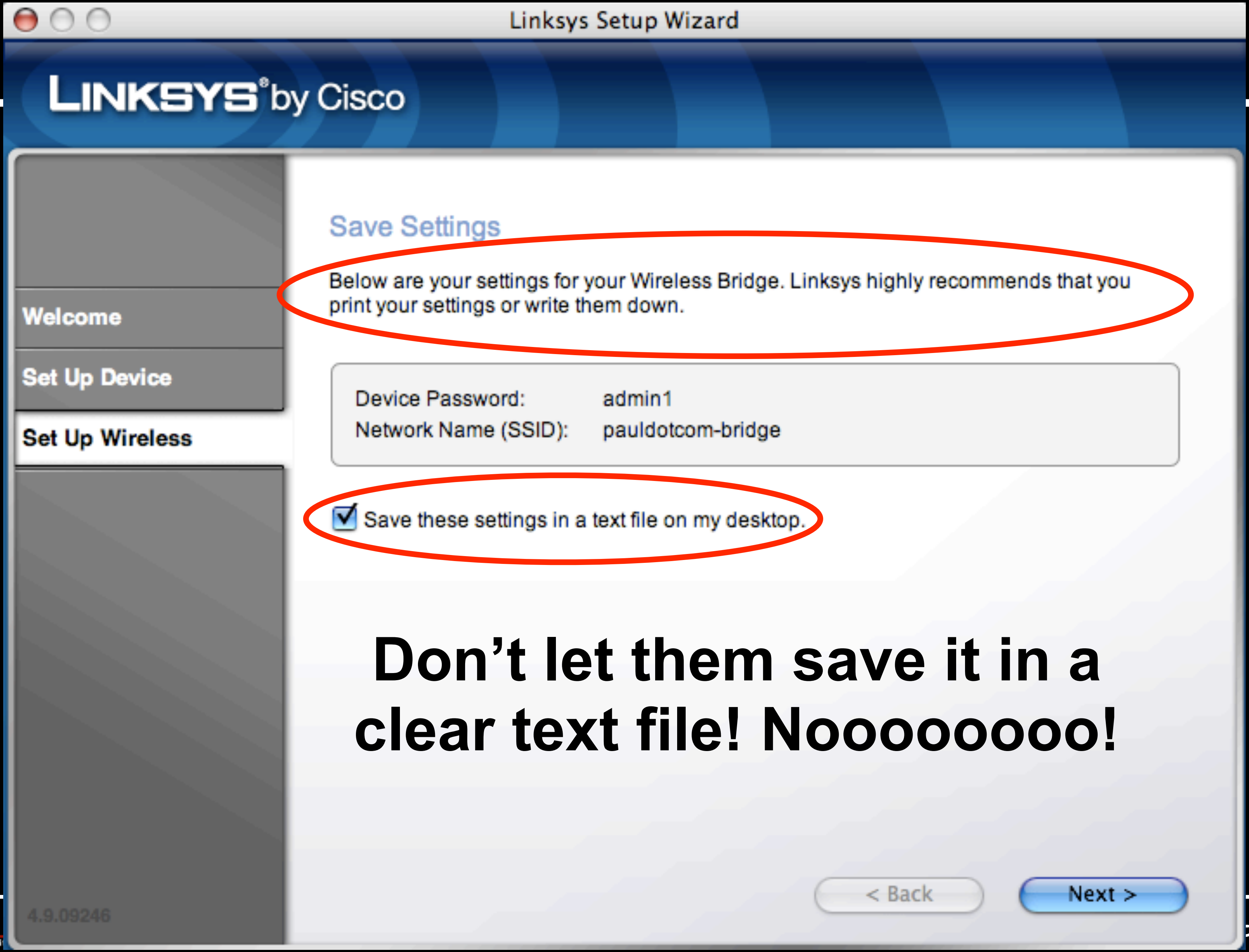
Password: admin

Learn more about device passwords

The new password must be different from the default password, which is "admin".

**WET610N setup program forces you to change the default password of "admin" to something different!**

# EPIC ~~WIN~~ FAIL!



Save Settings

Below are your settings for your Wireless Bridge. Linksys highly recommends that you print your settings or write them down.

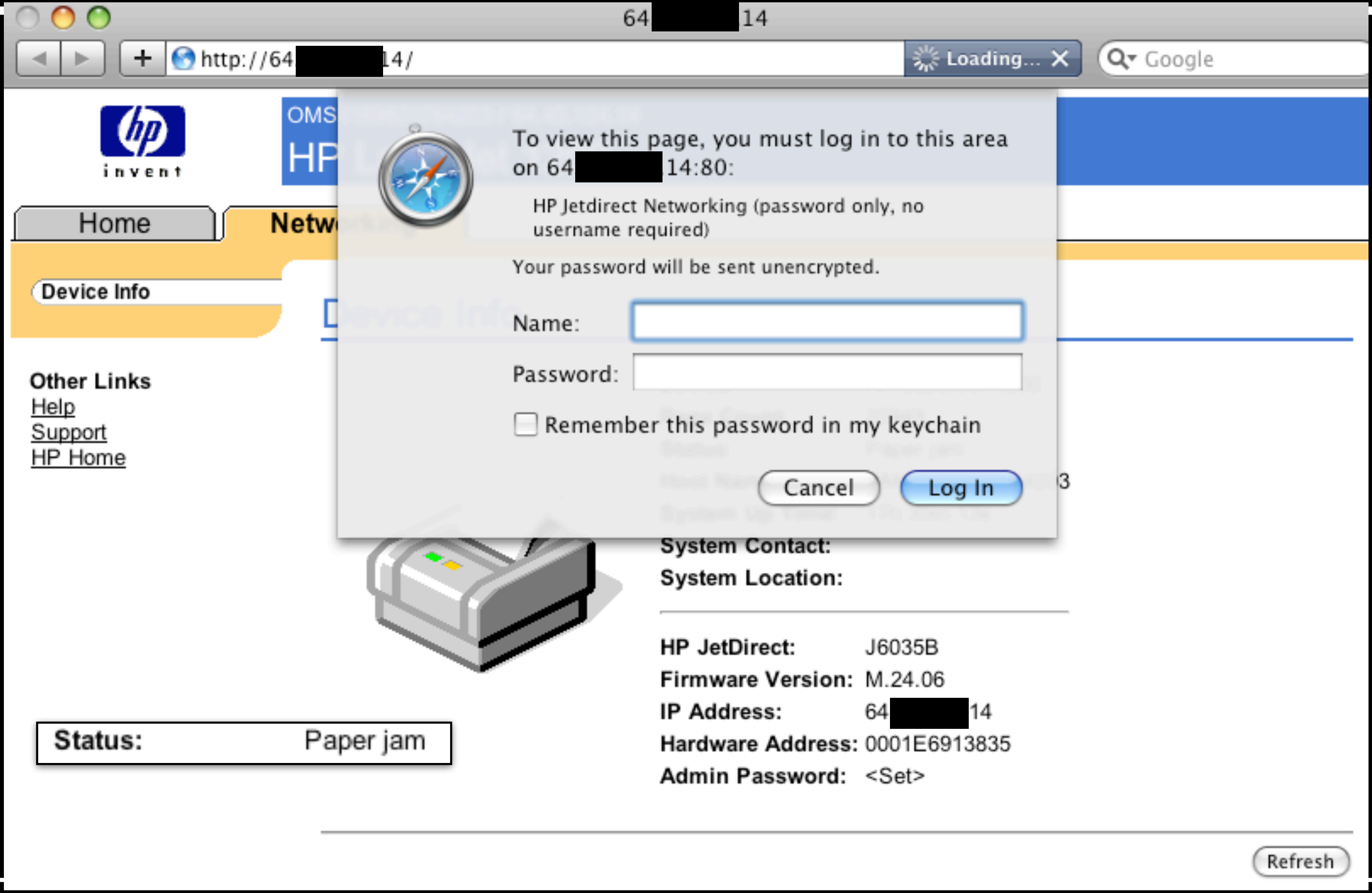
Device Password: admin1

Network Name (SSID): pauldotcom-bridge

☑ Save these settings in a text file on my desktop.

**Don't let them save it in a clear text file! Noooooooo!**

# Can we at least get a USERNAME with a password!



64[redacted]14

http://64[redacted]14/

To view this page, you must log in to this area on 64[redacted]14:80:

HP Jetdirect Networking (password only, no username required)

Your password will be sent unencrypted.

Name:

Password:

□ Remember this password in my keychain

System Contact:

System Location:

HP JetDirect: J6035B

Firmware Version: M.24.06

IP Address: 64[redacted]14

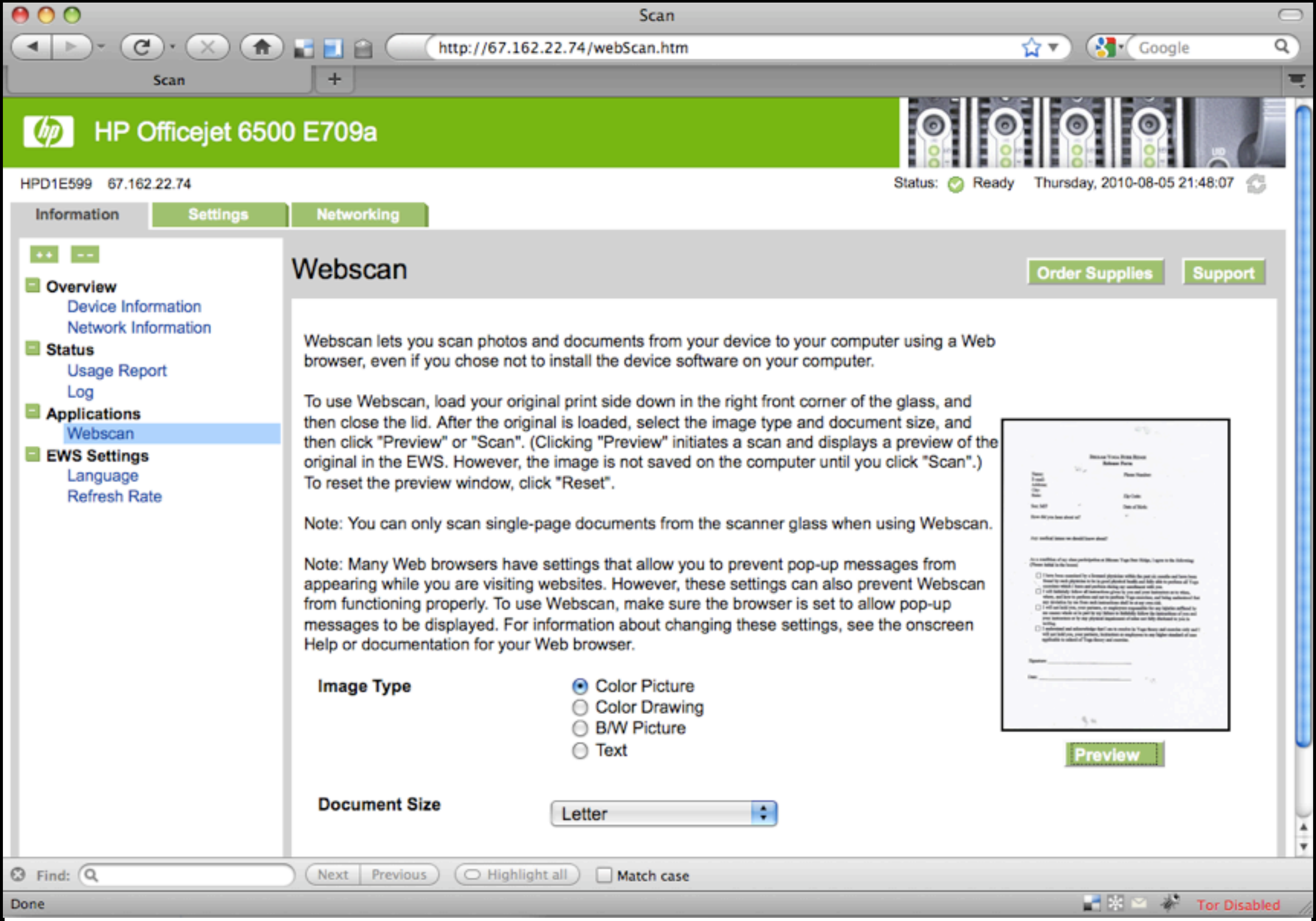
Hardware Address: 0001E6913835

Admin Password: <Set>

Status: Paper jam

# Multifunction Devices Do EVERYTHING

- Print, scan, fax, copy, email, wash my car, write my TPS reports, pick up the dry cleaning, bring me beer...
- Most devices can be accessed without authentication:
  - I tested this internally on a few networks
  - "Bob" tested this against millions of hosts on the Internet
- **Zscaler made a post as well:**
  - http://research.zscaler.com/2010/08/corporate-espionage-for-dummies-hp.html



HPD1E599 67.162.22.74

Status: Ready Thursday, 2010-08-05 21:48:07

## Webscan

Webscan lets you scan photos and documents from your device to your computer using a Web browser, even if you chose not to install the device software on your computer.

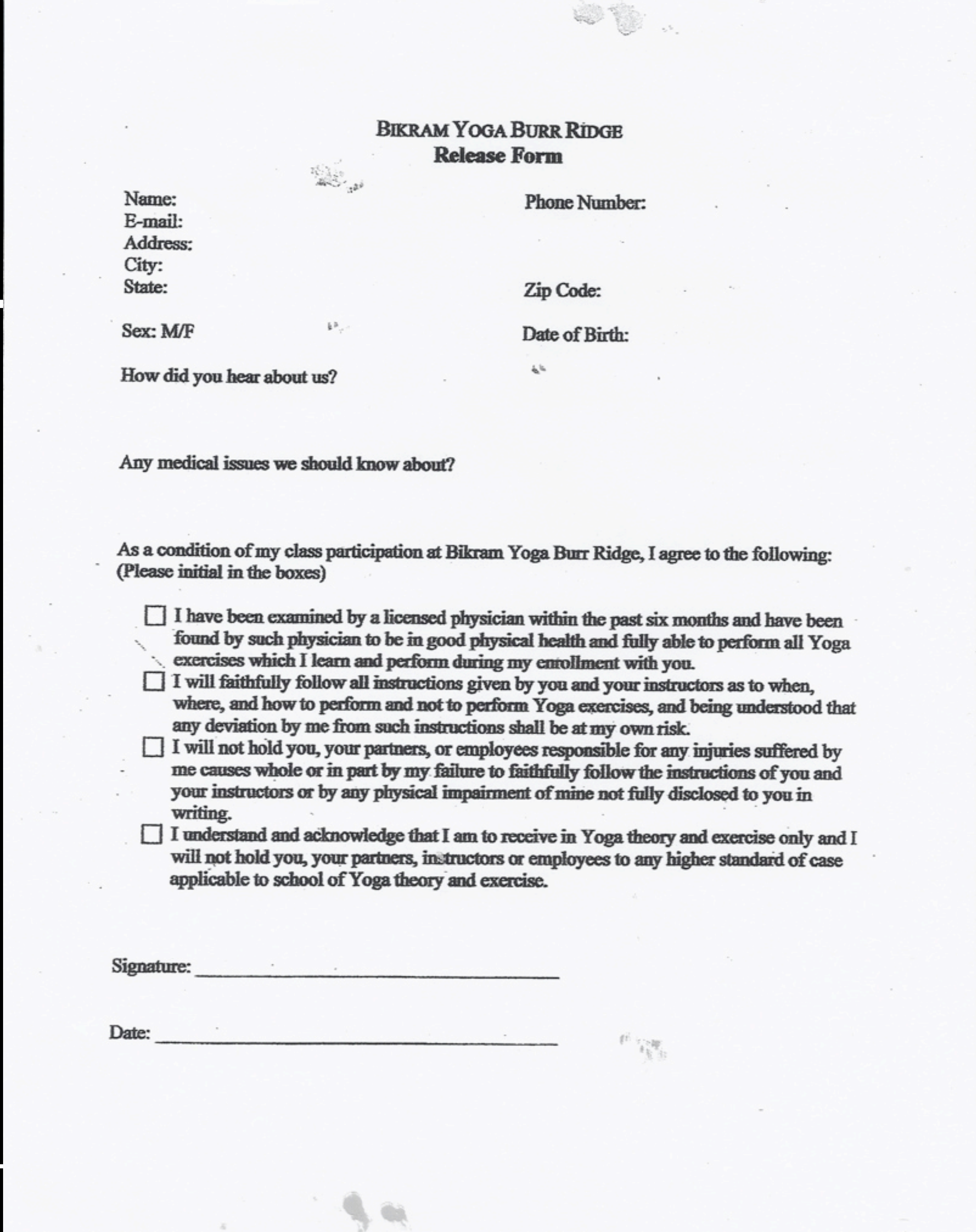
To use Webscan, load your original print side down in the right front corner of the glass, and then close the lid. After the original is loaded, select the image type and document size, and then click "Preview" or "Scan". (Clicking "Preview" initiates a scan and displays a preview of the original in the EWS. However, the image is not saved on the computer until you click "Scan".) To reset the preview window, click "Reset".

Note: You can only scan single-page documents from the scanner glass when using Webscan.

Note: Many Web browsers have settings that allow you to prevent pop-up messages from appearing while you are visiting websites. However, these settings can also prevent Webscan from functioning properly. To use Webscan, make sure the browser is set to allow pop-up messages to be displayed. For information about changing these settings, see the onscreen Help or documentation for your Web browser.

**Image Type**
● Color Picture
○ Color Drawing
○ B/W Picture
○ Text

**Document Size** Letter



BIKRAM YOGA BURR RIDGE
**Release Form**

Name:
E-mail:
Address:
City:
State:

Phone Number:

Zip Code:

Sex: M/F

Date of Birth:

How did you hear about us?

Any medical issues we should know about?

As a condition of my class participation at Bikram Yoga Burr Ridge, I agree to the following: (Please initial in the boxes)

□ I have been examined by a licensed physician within the past six months and have been found by such physician to be in good physical health and fully able to perform all Yoga exercises which I learn and perform during my enrollment with you.

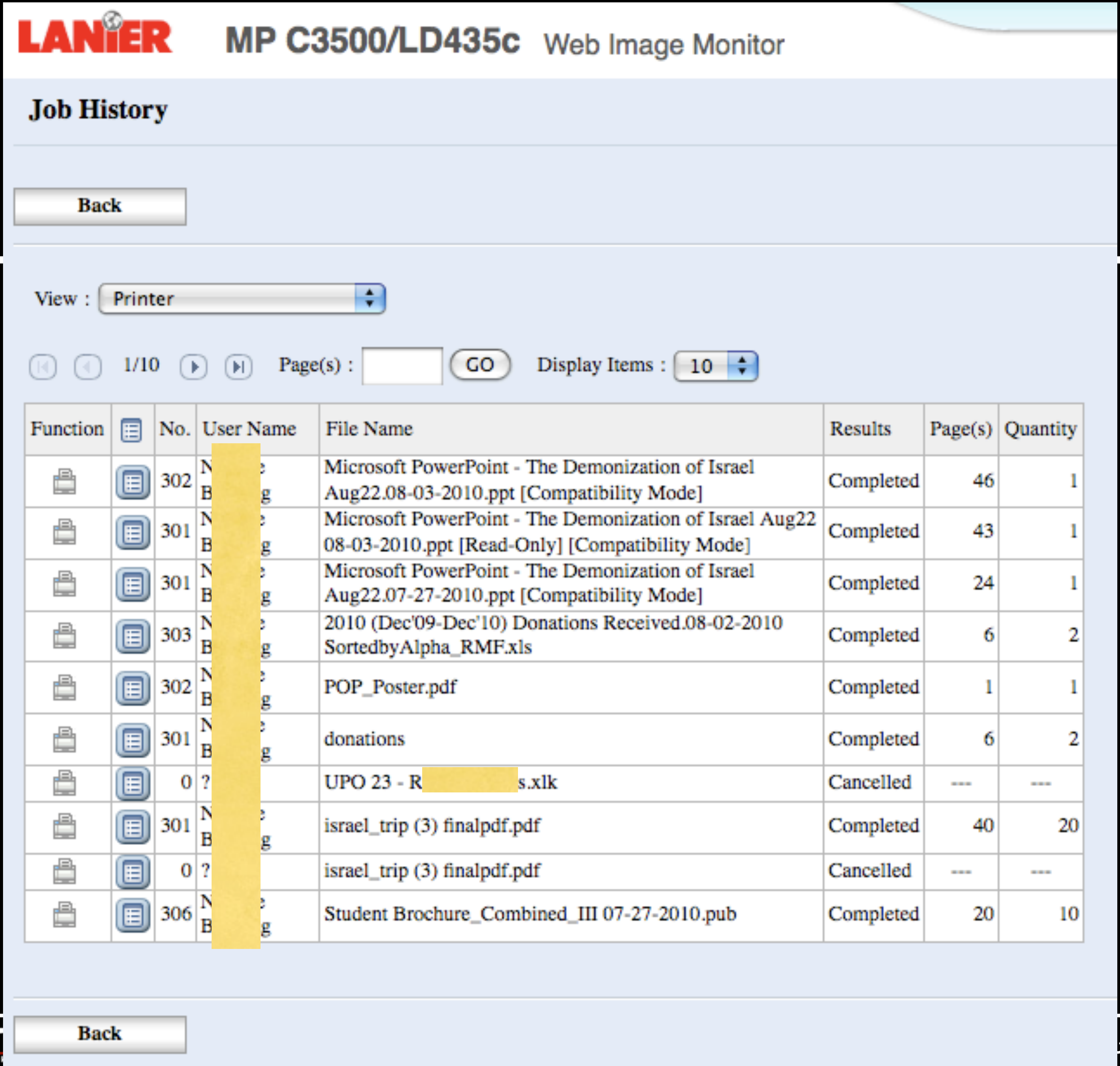
□ I will faithfully follow all instructions given by you and your instructors as to when, where, and how to perform and not to perform Yoga exercises, and being understood that any deviation by me from such instructions shall be at my own risk.

□ I will not hold you, your partners, or employees responsible for any injuries suffered by me causes whole or in part by my failure to faithfully follow the instructions of you and your instructors or by any physical impairment of mine not fully disclosed to you in writing.

□ I understand and acknowledge that I am to receive in Yoga theory and exercise only and I will not hold you, your partners, instructors or employees to any higher standard of case applicable to school of Yoga theory and exercise.

Signature: ______________________________

Date: ______________________________



LANIER MP C3500/LD435c Web Image Monitor

## Job History

Back

View : Printer

1/10 Page(s) : GO Display Items : 10

| Function | | No. | User Name | File Name | Results | Page(s) | Quantity |
|---|---|---|---|---|---|---|---|
| | | 302 | [redacted] | Microsoft PowerPoint - The Demonization of Israel Aug22.08-03-2010.ppt [Compatibility Mode] | Completed | 46 | 1 |
| | | 301 | [redacted] | Microsoft PowerPoint - The Demonization of Israel Aug22 08-03-2010.ppt [Read-Only] [Compatibility Mode] | Completed | 43 | 1 |
| | | 301 | [redacted] | Microsoft PowerPoint - The Demonization of Israel Aug22.07-27-2010.ppt [Compatibility Mode] | Completed | 24 | 1 |
| | | 303 | [redacted] | 2010 (Dec'09-Dec'10) Donations Received.08-02-2010 SortedbyAlpha_RMF.xls | Completed | 6 | 2 |
| | | 302 | [redacted] | POP_Poster.pdf | Completed | 1 | 1 |
| | | 301 | [redacted] | donations | Completed | 6 | 2 |
| | | 0 | ? [redacted] | UPO 23 - R[redacted]s.xlk | Cancelled | --- | --- |
| | | 301 | [redacted] | israel_trip (3) finalpdf.pdf | Completed | 40 | 20 |
| | | 0 | ? [redacted] | israel_trip (3) finalpdf.pdf | Cancelled | --- | --- |
| | | 306 | [redacted] | Student Brochure_Combined_III 07-27-2010.pub | Completed | 20 | 10 |

Back

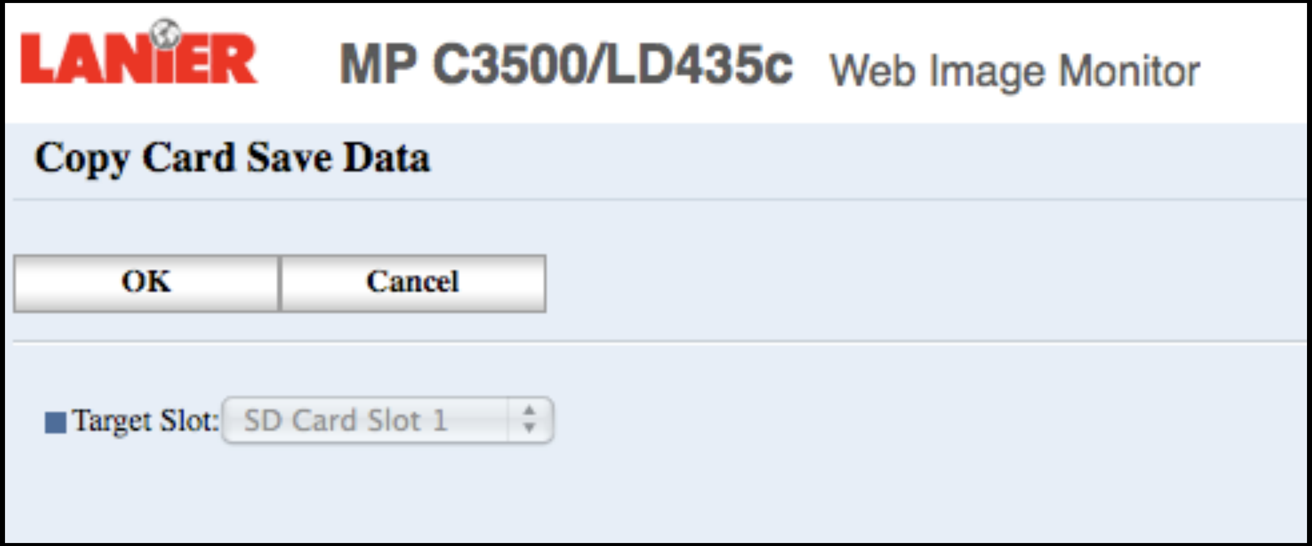
# Someone left a printer exposed to the Internet and now I know....

[WITH A LITTLE HELP FROM GOOGLE]

- The person's name, where they work, which department they work in
- Their area of study (Jewish studies)
- Potentially when they are taking a trip
- What applications they run (Powerpoint, Excel, PDF reader, MS Publisher)
  - Not the same version of Powerpoint that created the document
- They accept donations & promote Isreal
- UPO-23 = Electronic Hourly Employee Timecard for student mentor

# Can I have your USB stick?

- Yes.



LANIER MP C3500/LD435c Web Image Monitor

Copy Card Save Data

Target Slot: SD Card Slot 1

# Roku

```
press up
press down
press left
press right
press select
press home
press fwd
press back
press pause
```

```
# nc 192.168.1.240 8080
D0C9DP009064
ETHMAC 00:0d:4b:4c:29:5e
WIFIMAC 00:0d:4b:4c:29:5f
>
```

http://forums.roku.com/viewtopic.php?t=20106&sid=f0702e3bbba722ac7f1a59307209782c

# World Domination Propaganda

http://www.i-hacked.com/content/view/274/48/

# Even More Attacks

- HD Moore found several flaws in VxWorks, scanned 3.1 billion IP addresses and found 250,000 systems exposed to the Internet
  - http://blog.metasploit.com/2010/08/vxworks-vulnerabilities.html

- Craig Heffner discovered a DNS rebinding attack on several routers allowing attackers to gain control of administrative interfaces
  - http://code.google.com/p/rebind/

# Even More Attacks (2)

- Ki-Chan Ahn and Dong-Joo Ha created malware for Nintendo Wii and DS systems
  - http://games.venturebeat.com/2010/07/31/live-demos-of-hacking-the-nintendo-ds-and-the-wii-to-spread-malware/
- Barnaby Jack remotely attacked two different ATMs and “made the money come out” (without a card+pin #)
  - http://www.youtube.com/watch?v=qwMuMSPW3bU

# Potential Linksys Vulnerability

- Reported to Cisco PSIRT Feb 17, 2010
- **HNAP request can crash admin web server on certain models with certain firmware versions**
- Low impact vulnerability discovered by accident while trying to send a valid request
- The HNAP request format was taken directly from Cisco’s own documentation

# Curl Rules

```
curl http://192.168.1.70:80/HNAP1/ -v --basic \

--user  admin:admin -H \

'SOAPAction: "http://purenetworks.com/HNAP1/
GetWLanRadioSecurity"' \

--data @xml/GetWLanRadioSecurity.xml
```

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope>
<soap:Body>
<GetWLanRadioSecurity xmlns="http://purenetworks.com/HNAP1/" />
</soap:Body>
</soap:Envelope>
```

# Lame?

- Turns out to not be reproducible (my router was a DD-WRT upgrade)
- Certainly lame.  However shows just how fragile these devices and protocols are
- What would happen if you were to actually fuzz HNAP?
- Release notes of firmware running on device say “Fixed HNAP issue”
- **However, there is no way to disable HNAP**

# But Seriously, What Do We Do About It?

- I can show you embedded systems security fail until you are tired of hearing about it (which was probably 15 minutes ago or longer)
- I could go out and find more vulnerabilities and talk about them
- Some problems are implementation-based, nevermind a 0day (e.g. no HNAP disable)
- So how do we fix it?

**www.securityfail.com**

# www.securityfail.com

- Used to redirect to ww.grc.com (Gigidy)
- It is now a public Wiki where people can write mini-articles on security failures
- First major section will be dedicated to embedded systems
- Write-in about how embedded security has failed you
  - 0Days are okay too, but not sure that will help
- Raise awareness and work to change the industry to implement better security on devices

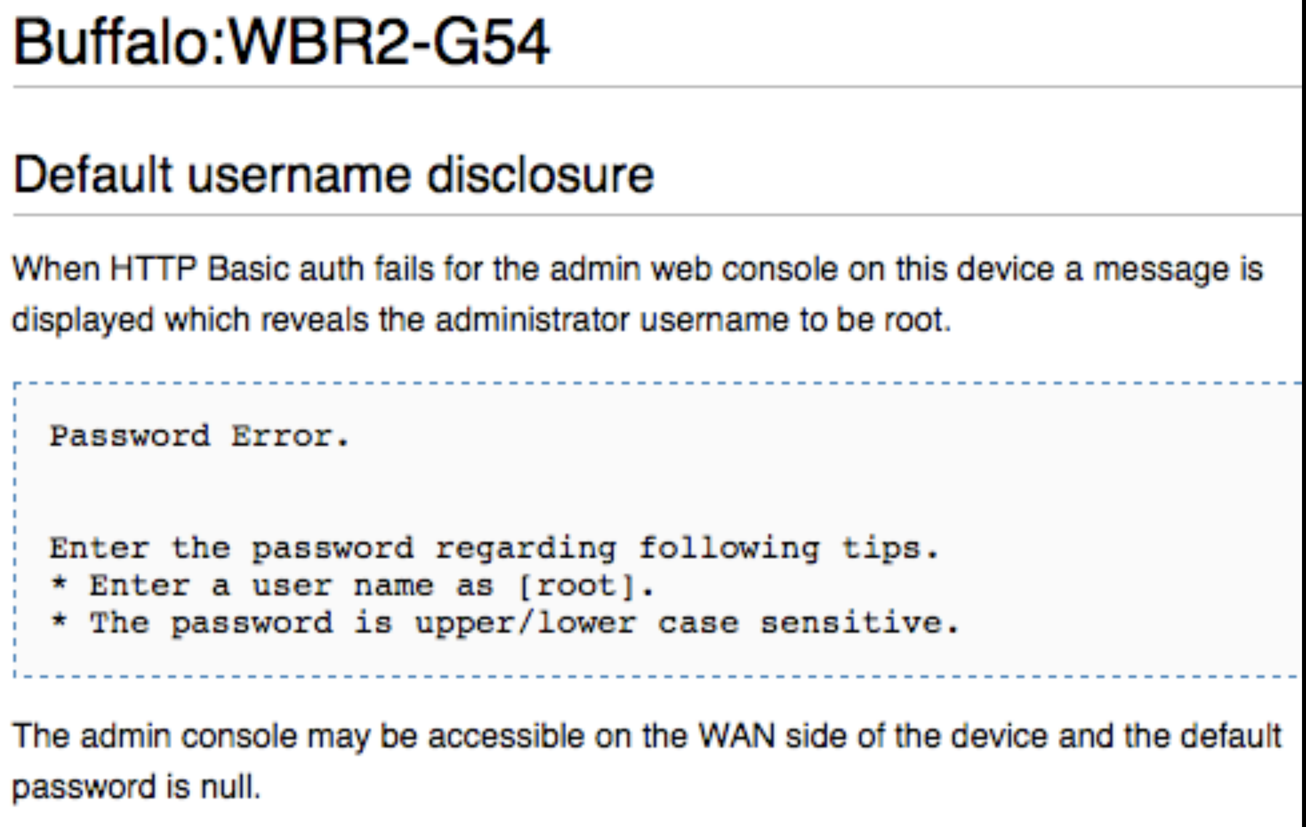
# www.securityfail.com

## Some GOALS to get us started:

- We want vendors of embedded systems to:
  - FORCE the user to select the password
  - Allow users to disable protocols
  - Only enable secure management protocols by default (HTTPS, SSH)
- We want ISPs to:
  - Block inbound port 80 on user subnets
  - Manage customer devices properly and implement security

# Sign up for an account

- Email me if you want an account in the mean time
- Or just send me your stories anonymously
- **This is a non-profit project**
  - Its sole purpose is to raise awareness and hopefully work with the industry to change



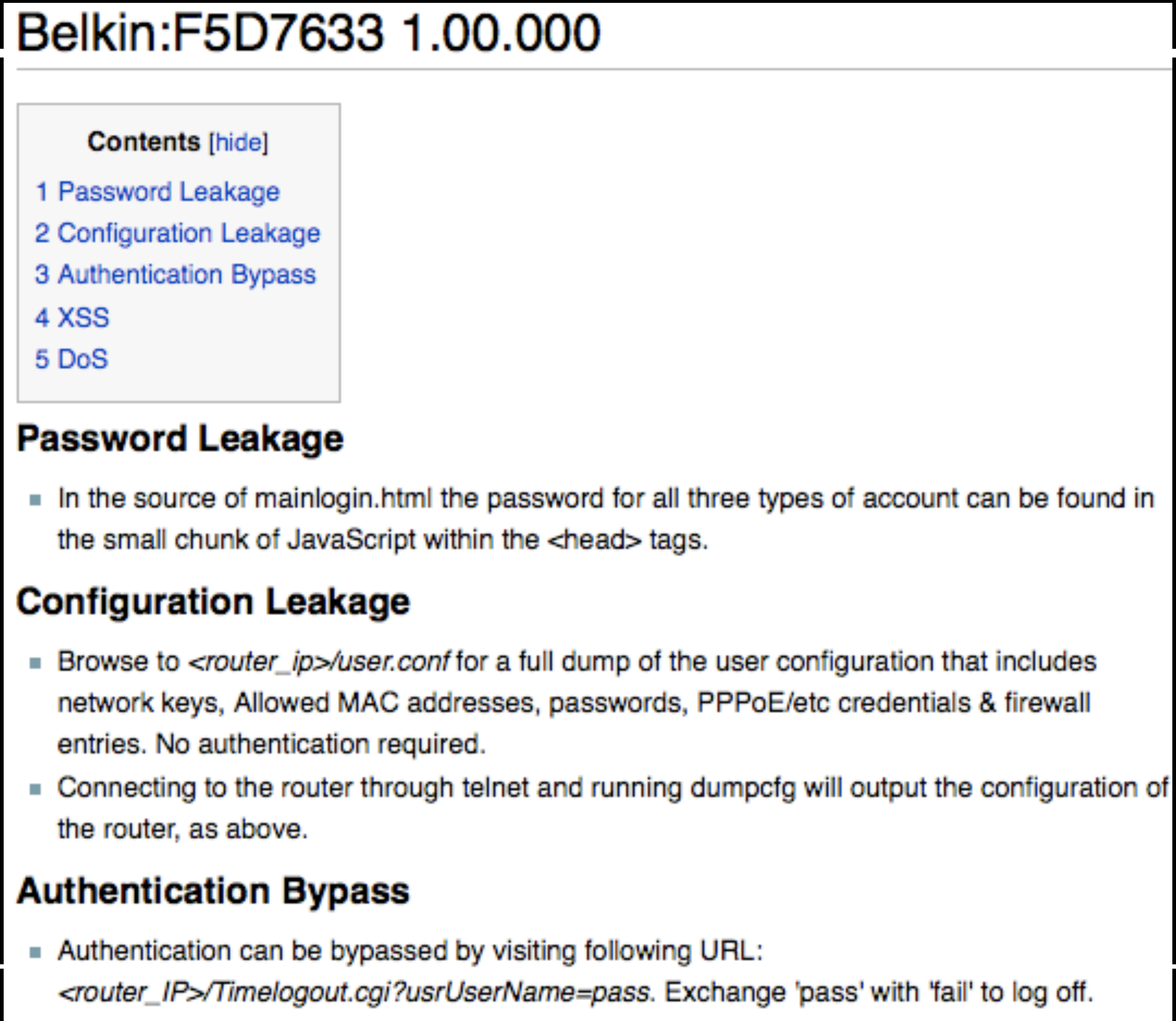
# Buffalo:WBR2-G54

## Default username disclosure

When HTTP Basic auth fails for the admin web console on this device a message is displayed which reveals the administrator username to be root.

```
Password Error.


Enter the password regarding following tips.
* Enter a user name as [root].
* The password is upper/lower case sensitive.
```

The admin console may be accessible on the WAN side of the device and the default password is null.



# Belkin:F5D7633 1.00.000

Contents [hide]

## Password Leakage

- In the source of mainlogin.html the password for all three types of account can be found in the small chunk of JavaScript within the <head> tags.

## Configuration Leakage

- Browse to *<router_ip>/user.conf* for a full dump of the user configuration that includes network keys, Allowed MAC addresses, passwords, PPPoE/etc credentials & firewall entries. No authentication required.
- Connecting to the router through telnet and running dumpcfg will output the configuration of the router, as above.

## Authentication Bypass

- Authentication can be bypassed by visiting following URL: *<router_IP>/Timelogout.cgi?usrUserName=pass*. Exchange 'pass' with 'fail' to log off.

# So what about World Domination?

# Things I wanted to cover but ran out of space

- The “Chuck Norris” worm, which could a version of the psyb0t?
- Static analysis of device firmware, mounting the filesystems, finding vulnerabilities
- Analyzing video game systems, Tivo, and Blue-Ray players as they are network connected
- Wireless type worms and default Wifi settings
- Segmentation is just a band-aid

# Don’t Forget:
# http://www.securityfail.com

- **Presentations:** http://pauldotcom.com/presentations.html
- **Radio:** http://pauldotcom.com/radio
- **Live Stream:** http://pauldotcom.com/live
- **Forum:** http://forum.pauldotcom.com/
- **Mailing List:** http://mail.pauldotcom.com
- **Webcasts:** http://pauldotcom.com/webcasts
- **Insider:** http://pauldotcom.com/insider
- **Email:** psw@pauldotcom.com