

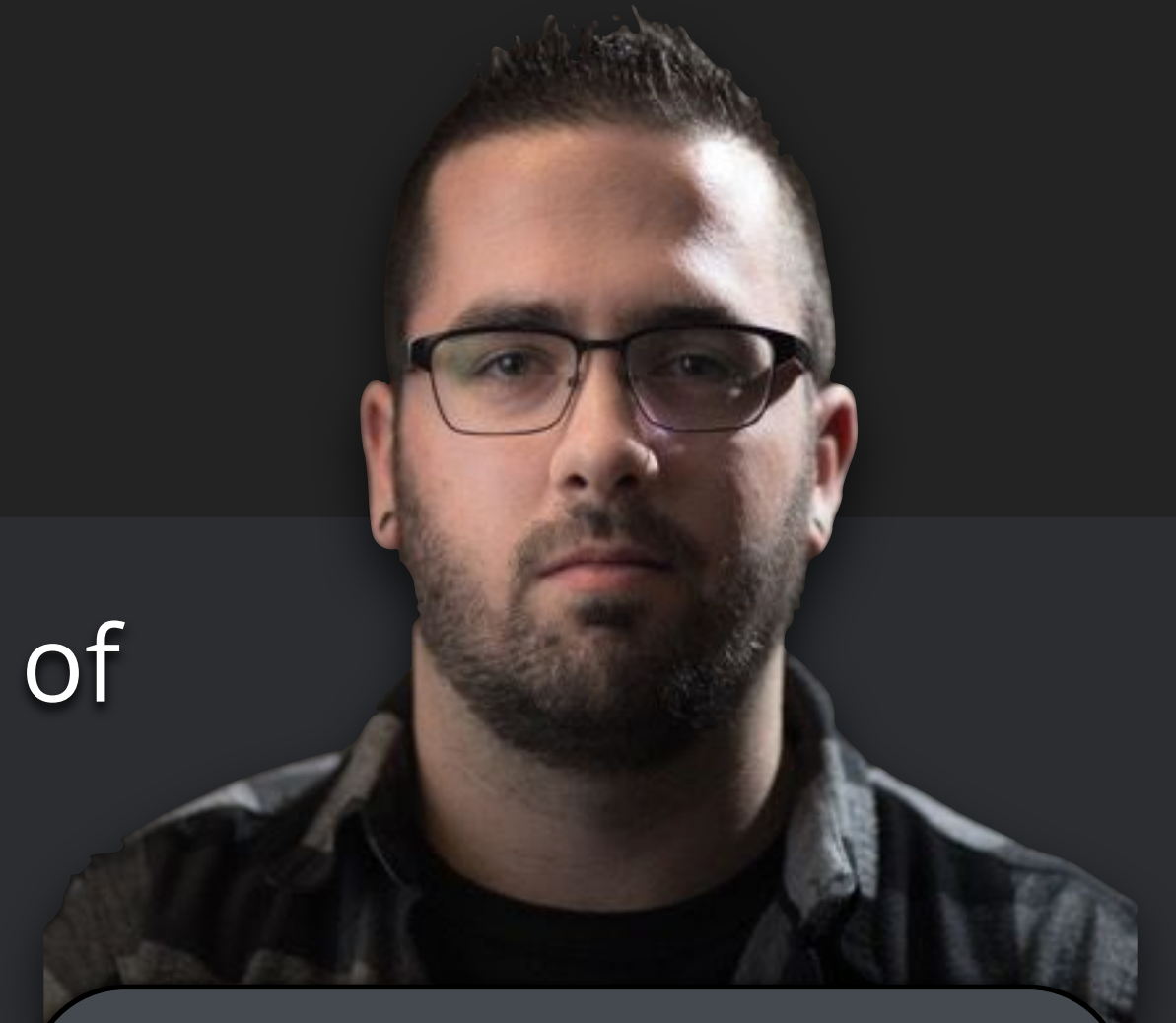



IoT in 2016: *a serious overview of IoT today and a technical preview of HoneyVNC*

By Yonathan Klijnsma

Yonathan Klijnsma




Senior Threat Intelligence Analyst



Perform threat intelligence analysis at  **FOX IT** keeping track of current events and work on new upcoming threats.

I do my part in:

- Malware analysis (reverse engineering)
- Network Forensics
- Programming

 @ydklijnsma
 github.com/0x3a
 blog.0x3a.com

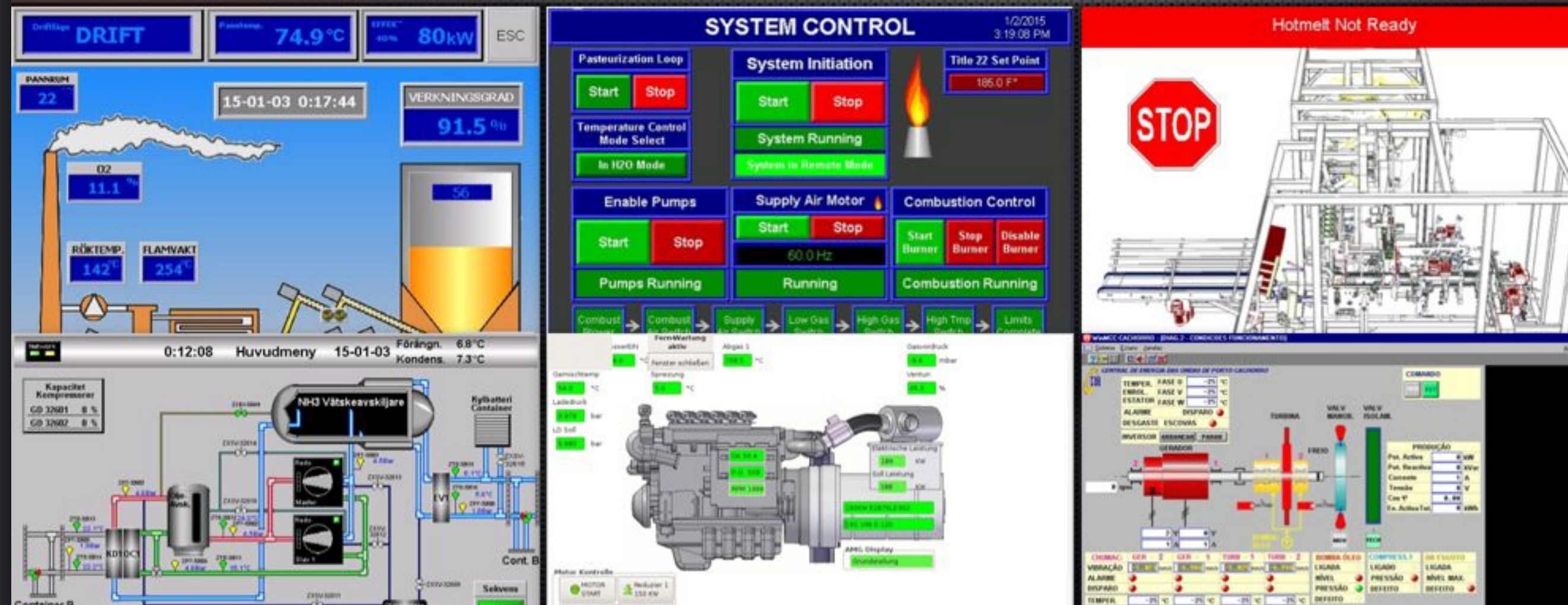
Besides \$DAYJOB I like to *'play around'* with security related things. This varies from malware analysis to random programming projects ending in POC status 99% of the time.

I occasionally write about my findings on my blog.



FIRST TC Amsterdam 2015

Large industrial controllers for everyone!



The Internet: a fun place of interconnected devices
by Yonathan Klijnsma



FIRST TC Amsterdam 2015

Cheapest printing/faxing/scanning!

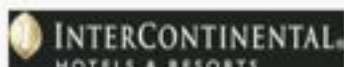
Cheapest: Marriot / Hyatt Hotels - 1\$



Swipe your credit card or press
Next to enter information manually.

Copies <small>(per page)</small>	Scan to Email <small>(per recipient)</small>	Faxes <small>(per recipient)</small>
B/W: \$0.15 Color: \$1.79	\$1.00	First page: \$1.00 Each add'l page: \$1.00



Most expensive: Intercontinental - 5.43\$





Swipe your credit card or press
Next to enter information manually.

Copies <small>(per page)</small>	Scan to Email <small>(per recipient)</small>	Faxes <small>(per recipient)</small>
B/W: \$0.27 Color: \$3.26	\$5.43	First page: \$4.34 Each add'l page: \$4.34

Random finds: Getting creepy



IP Location  United States Chicago James Crown
ASN  AS7922 COMCAST-7922 - Comcast Cable Communications, Inc. (registered Feb 14, 1997)



73-167-187-56-1

CustName:	JAMES CROWN
Address:	65 E GOETHE ST
City:	CHICAGO
StateProv:	IL
PostalCode:	60610
Country:	US
RegDate:	2012-05-31
Updated:	2013-02-02
Ref:	http://whois.arin.net/rest/customer/C02985897



It was getting pretty bad back then right?....



We were the firemen taking pictures with the small fires just smiling and laughing.



Did it get better?



No..



No.... no really



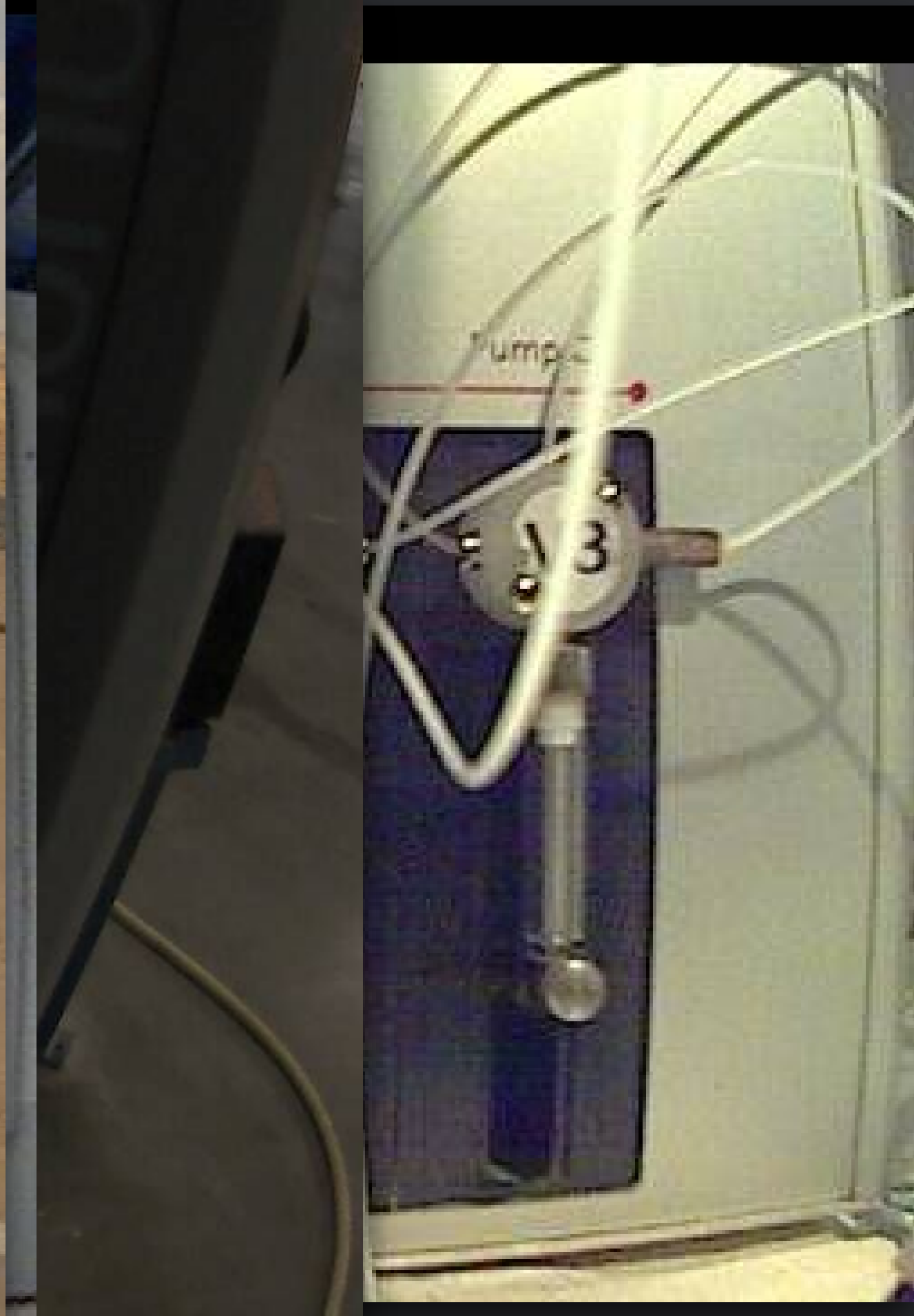
Its currently even worse...



It doesn't seem to get better...



Security Camera "IoT"



Security Camera “IoT”



Internet of Things Conference

The screenshot shows the homepage of the Internet of Things World 2016 conference website. The background is a blurred image of a crowd of people. At the top, there is a navigation menu with the following items: Home (house icon), CONFERENCE (dropdown arrow), EXHIBITION (dropdown arrow), SPONSOR & EXHIBIT (dropdown arrow), EVENT INFO (dropdown arrow), MEDIA & CONTENT (dropdown arrow), REGISTER (dropdown arrow), and GLOBAL SERIES (dropdown arrow). In the top right corner, there are social media icons for YouTube and LinkedIn. The main content area features the event logo on the left, which consists of the text "Internet of Things" in a large, bold, white font, with "WORLD" in a smaller font below it. To the right of the text is a colorful, abstract logo element. To the right of the logo, the text reads "NEW VENUE!" in bold white, followed by "May 10 - 12, 2016" in a larger blue font, and "Santa Clara Convention Center, Silicon Valley" in white. Below this, the text "The world's largest & most comprehensive IoT event" is displayed in white. A prominent pink button with the text "Download the Event Brochure" is centered below the main text. At the bottom of the page, there is a horizontal navigation bar with four items: "Hackathon", "Book a Stand", "Register for Conference", and "Register for Free Expo".

CONFERENCE ▾ EXHIBITION ▾ SPONSOR & EXHIBIT ▾ EVENT INFO ▾ MEDIA & CONTENT ▾ REGISTER ▾ GLOBAL SERIES ▾

Internet of Things
WORLD

NEW VENUE!
May 10 - 12, 2016
Santa Clara Convention Center,
Silicon Valley

The world's largest & most comprehensive IoT event

Download the Event Brochure

Hackathon Book a Stand Register for Conference Register for Free Expo



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'


 **Dan Tentler**
@Viss


... is this an exercise bike?!
shodan.io/host/128.171.2...



Workout Time: 20 minutes
RPM: 50

128.171.239.246
Ports open: 22, 5900

 **Yonathan Klijsma** @ydklijsma · 21 Dec 2015
@Viss this one is live! Someone is cycling :D shodan.io/host/128.171.2...



Progress View | Simple View | Track View | Heart View | Calories: 19 | Cal/Hour: 302 | Watts: 62

Level

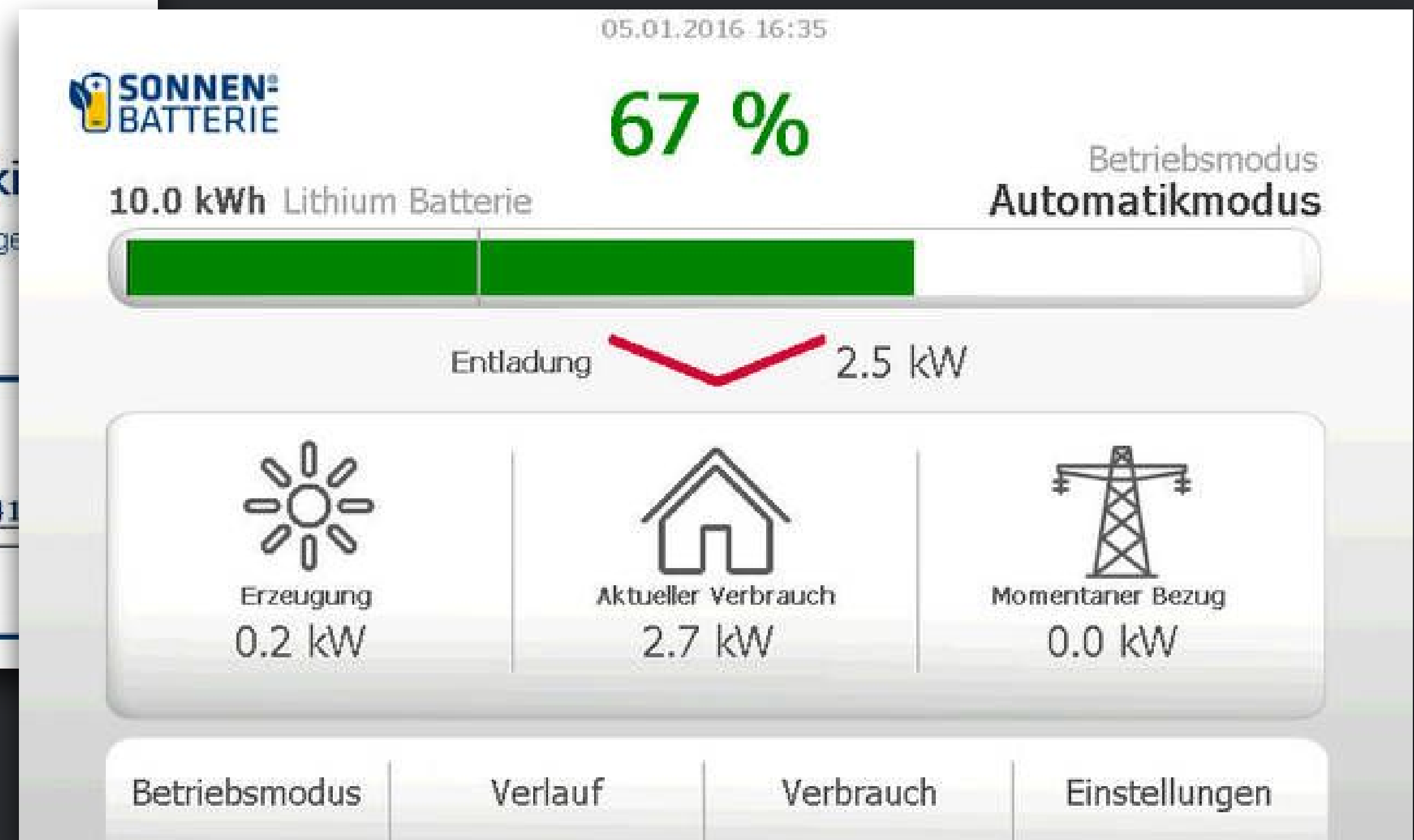
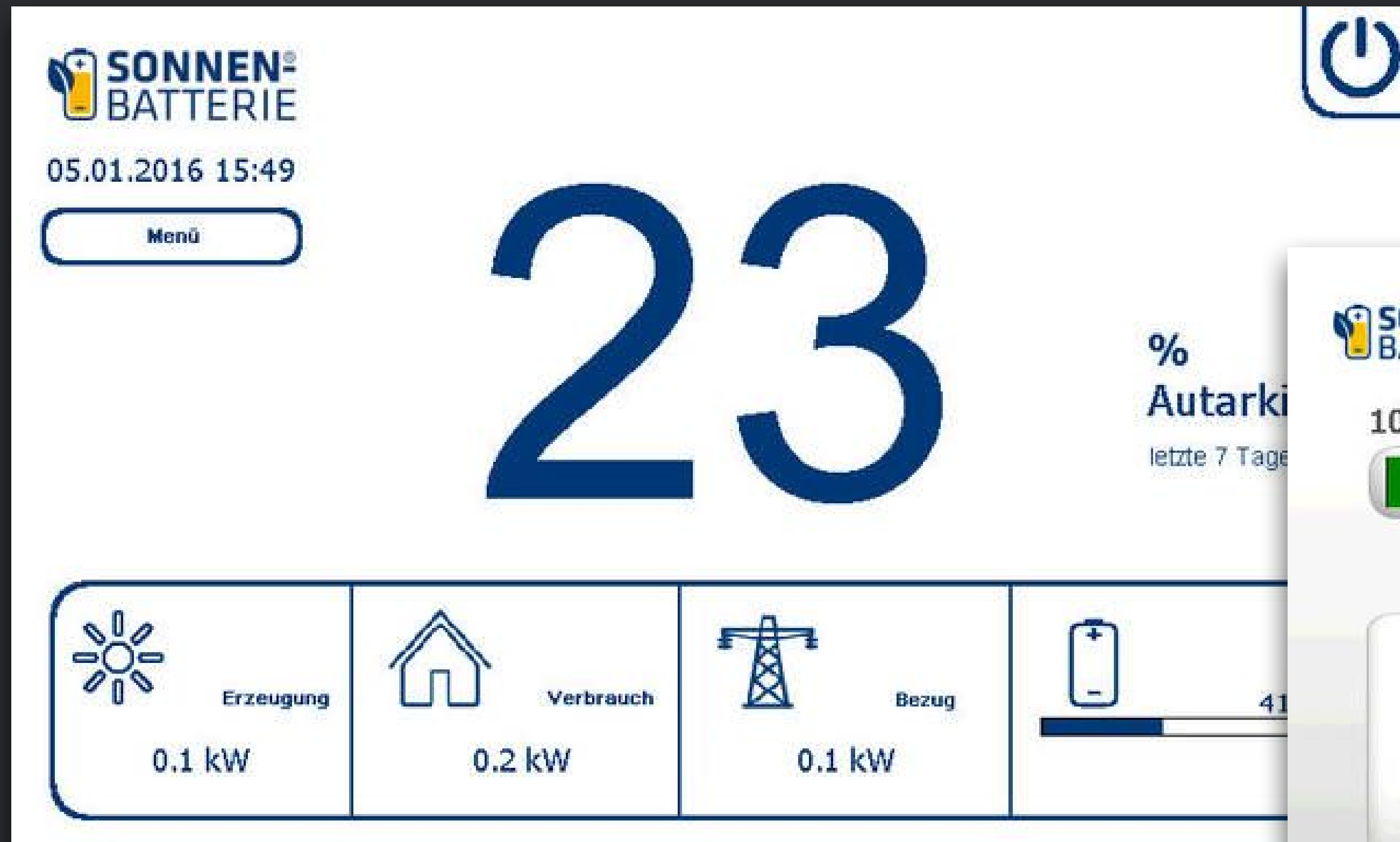
4:16 minutes
0.53 miles

Workout Time: 20 minutes | RPM: 33 | Level: 10

STAR TRAC ENTERTAINMENT | NOT SIGNED IN



German 'Sonnenbatterie' solar-cell power storage systems



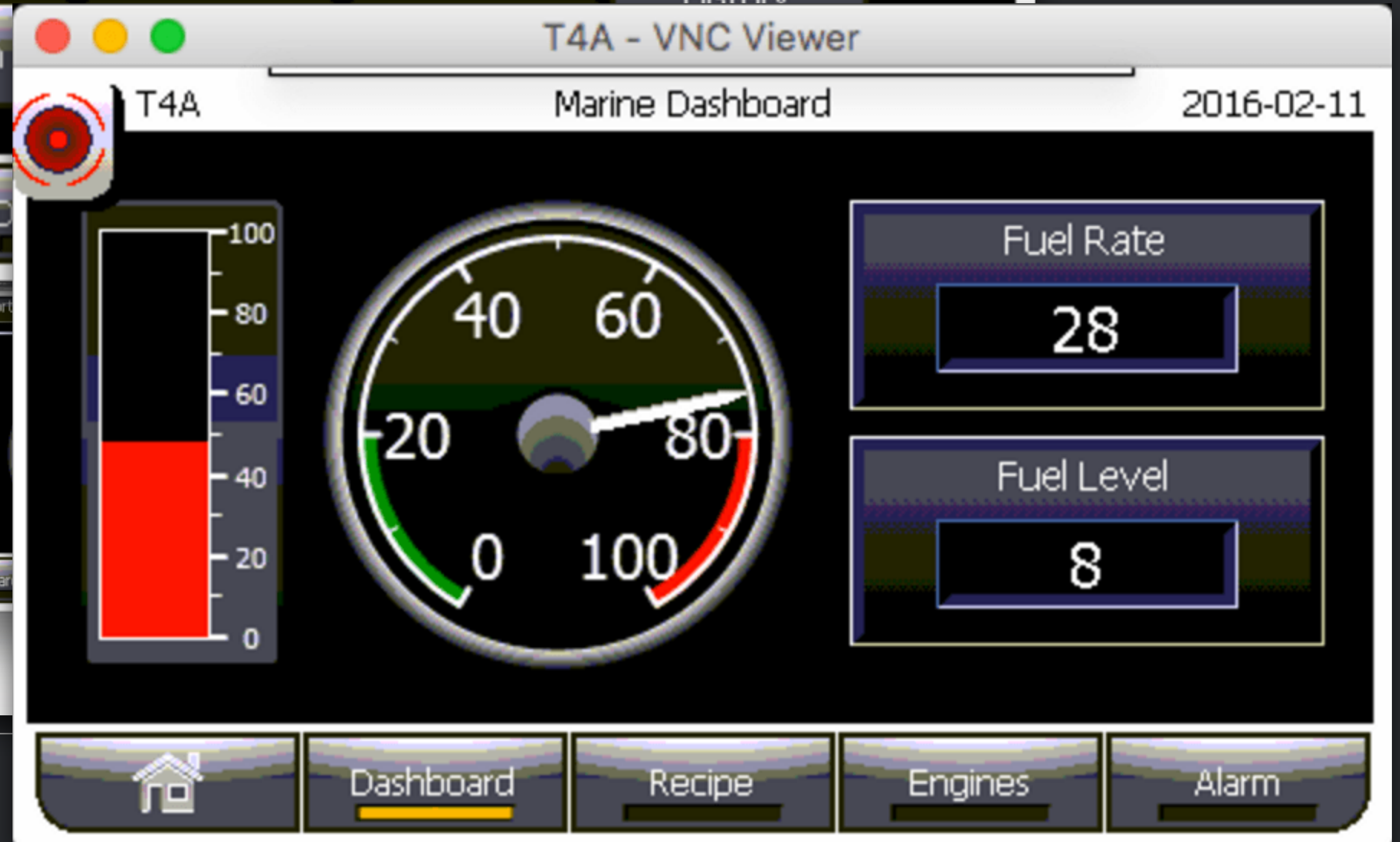
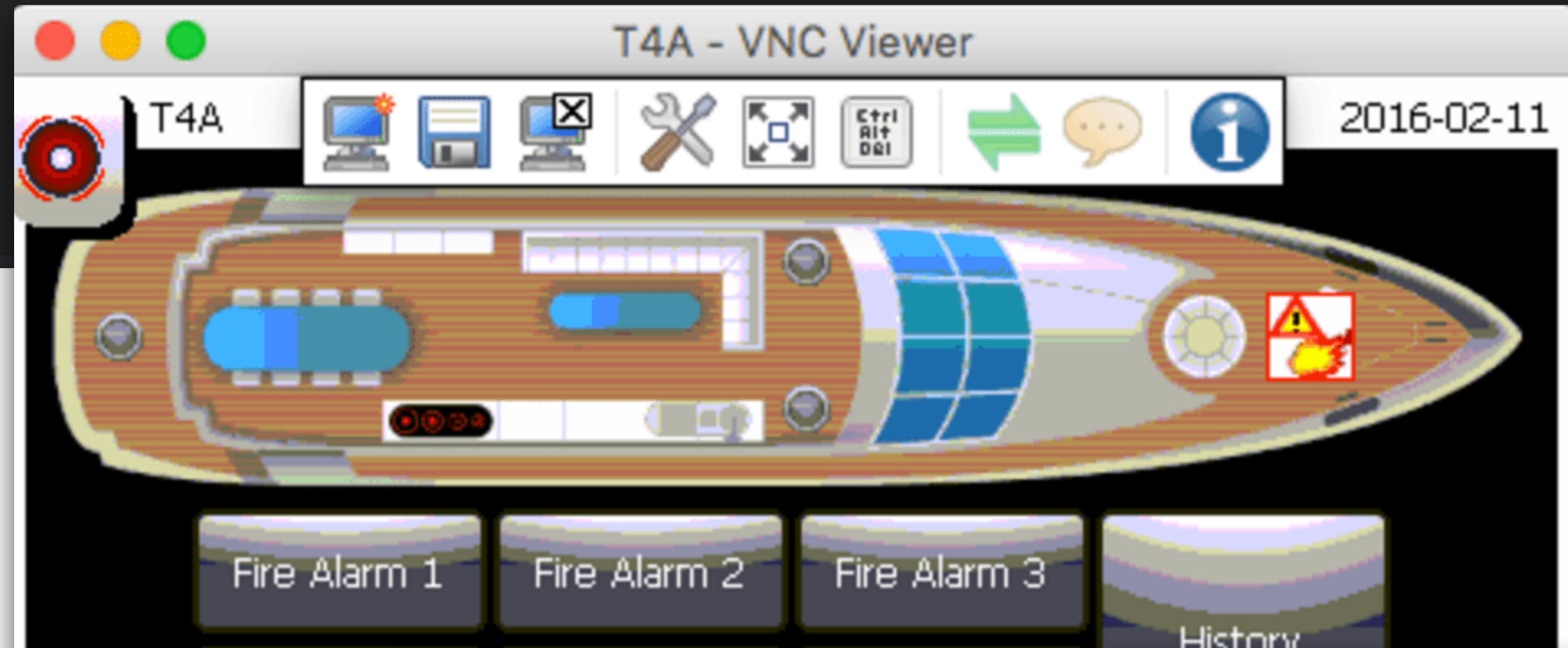
Boats...



Dan Tentler

@Viss

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



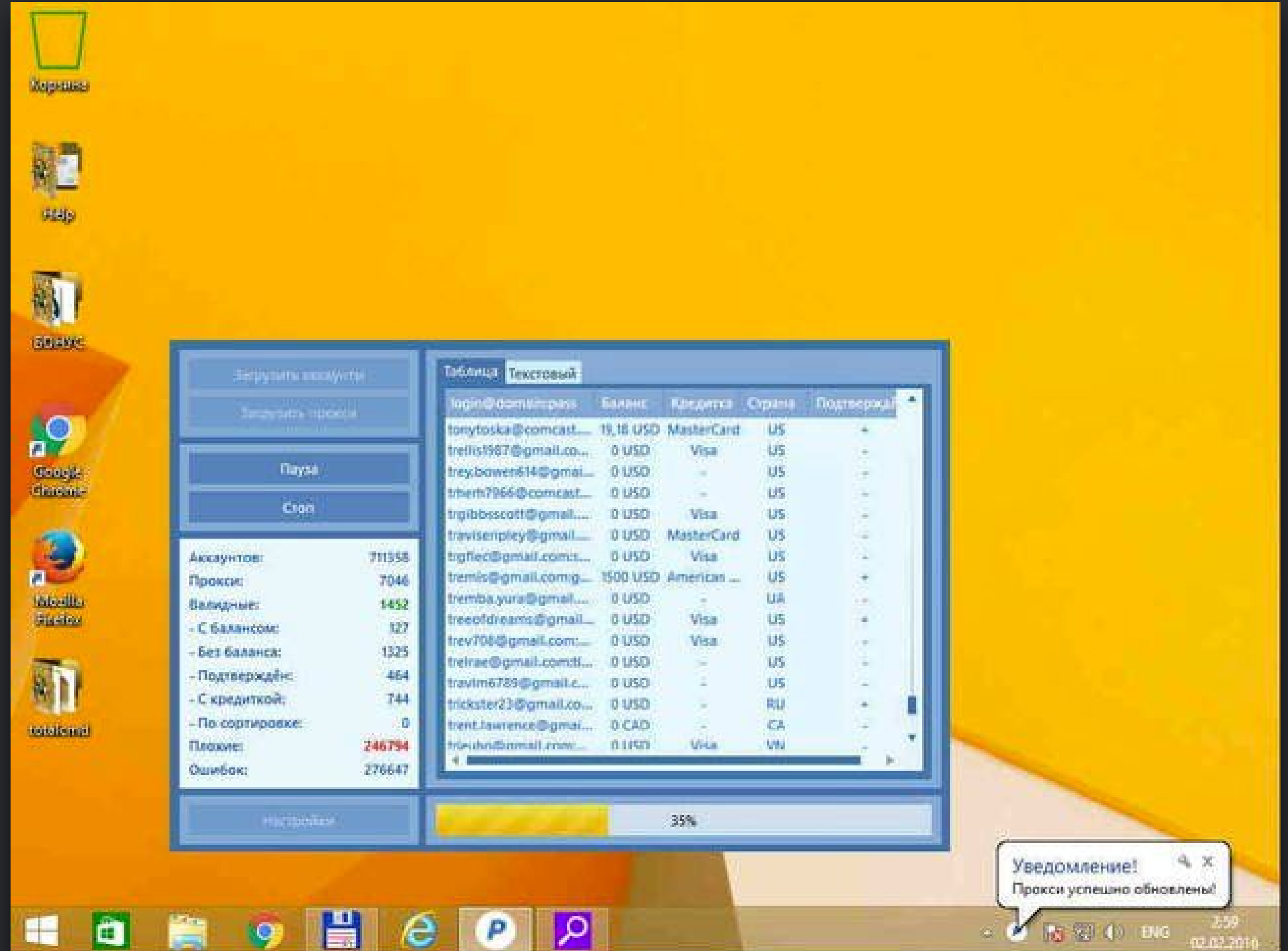
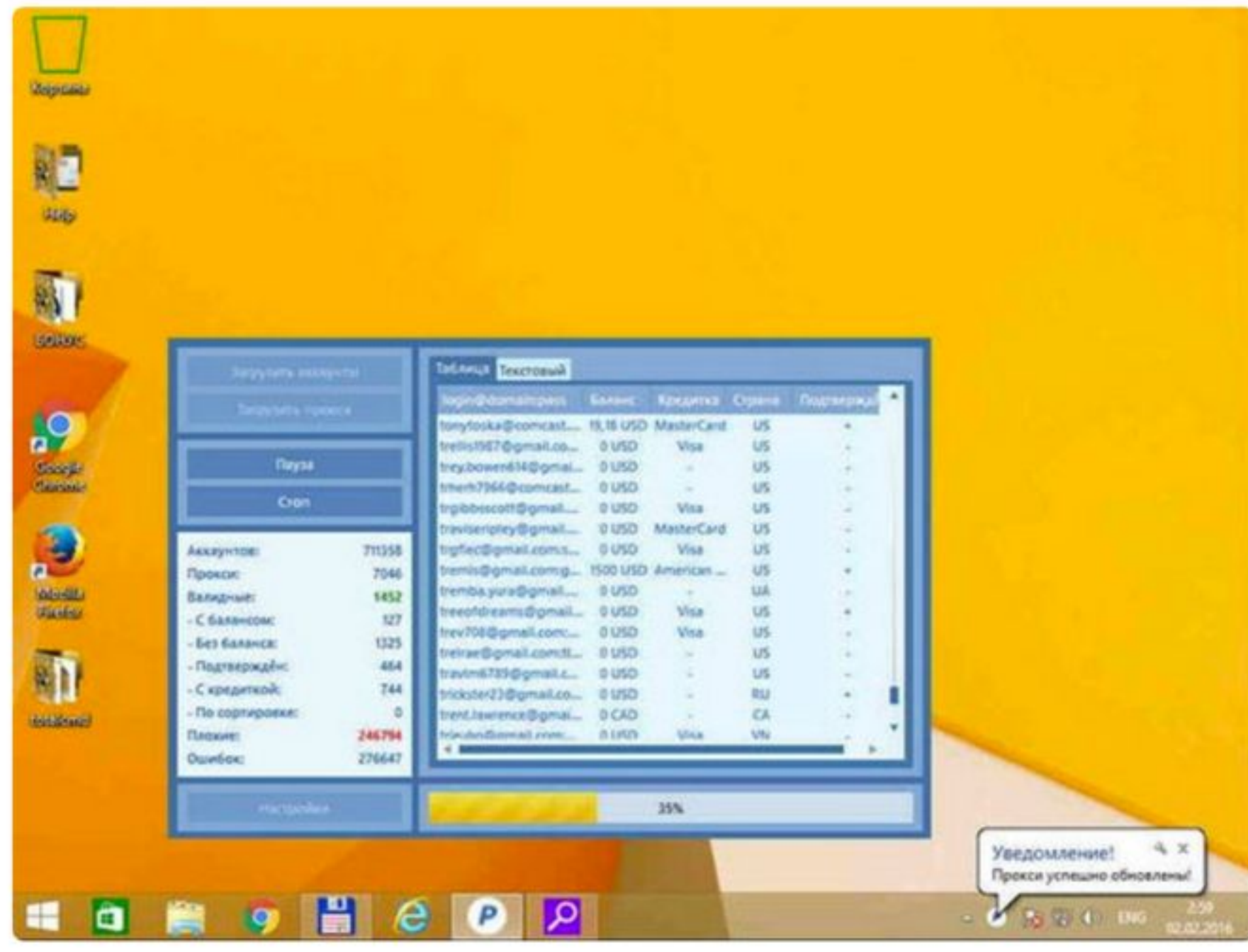
We can find criminals(!?) on VNC....



Yonathan Klijsma

@ydklijsma

Found open VNC on a server where a criminal was cashing out paypal accounts, talk about getting caught in the act...



Maldives fishes! :D



Dan Tentler
@Viss



Following

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

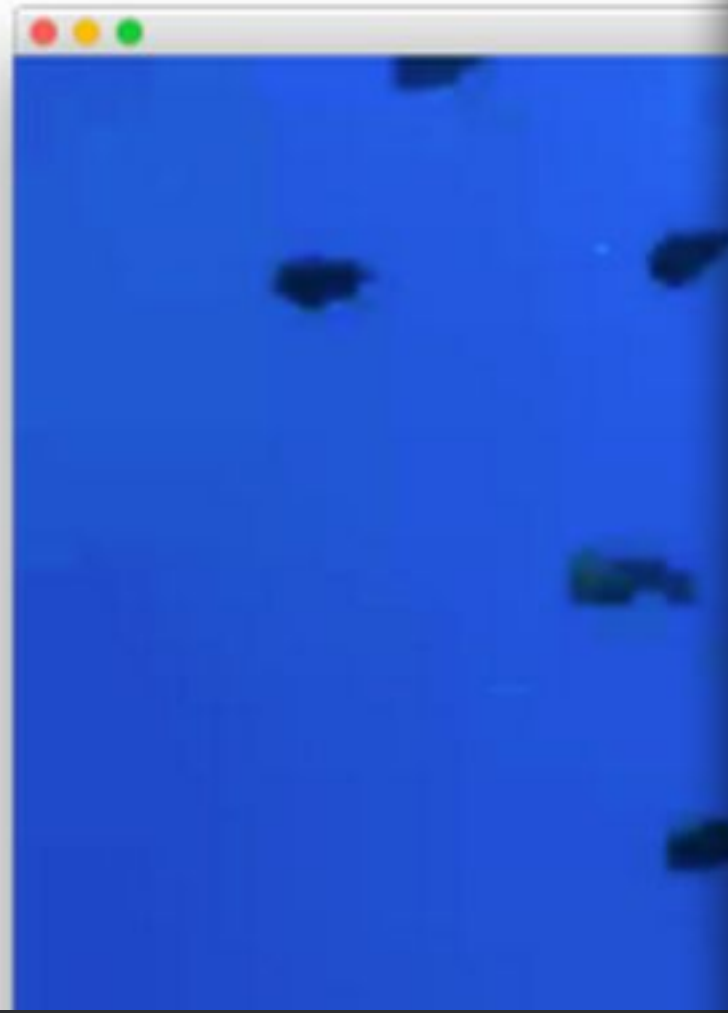
AUGH. I got back from flying, completely forgot I left this on.

Just about shit my pants



Dan Tentler
@Viss

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



Cardiac imaging on Shodan....

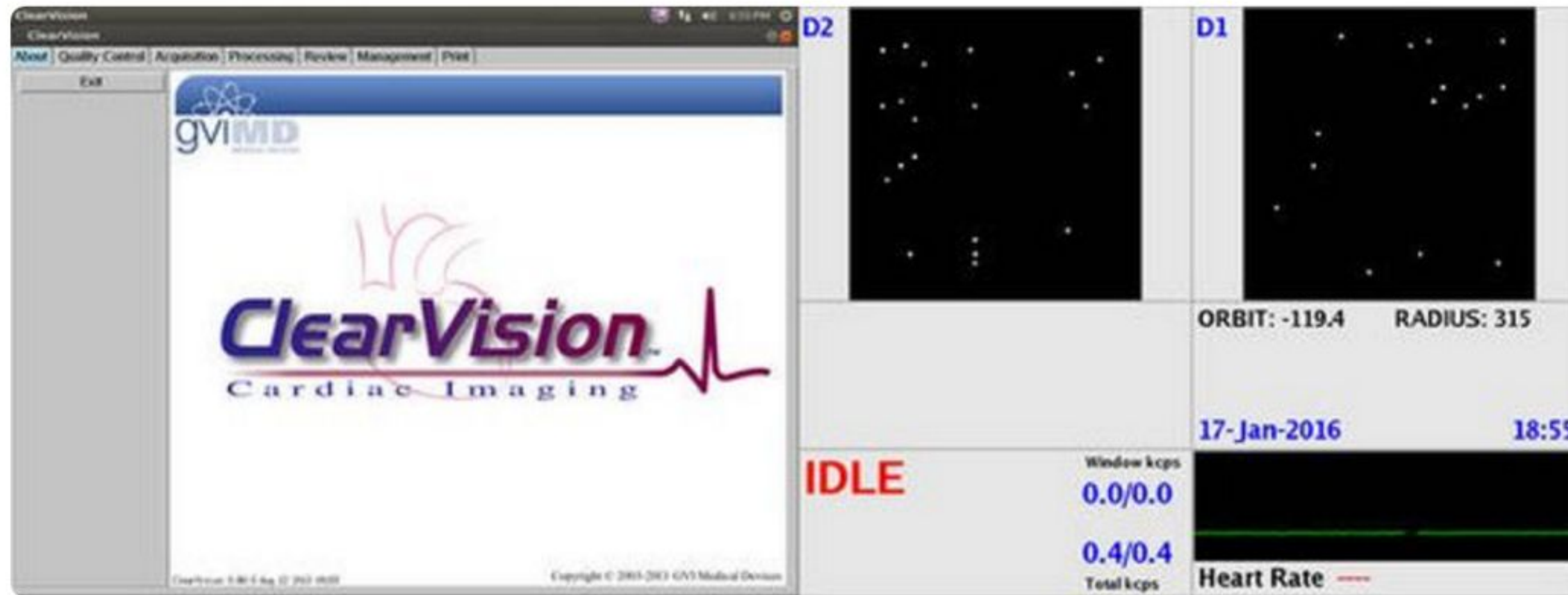


Yonathan Klijsma

@ydklijsma

More open & unauthenticated VNC on medical devices: a cardiac imaging device:

shodan.io/host/201.231.2... (cc @shodanhq)

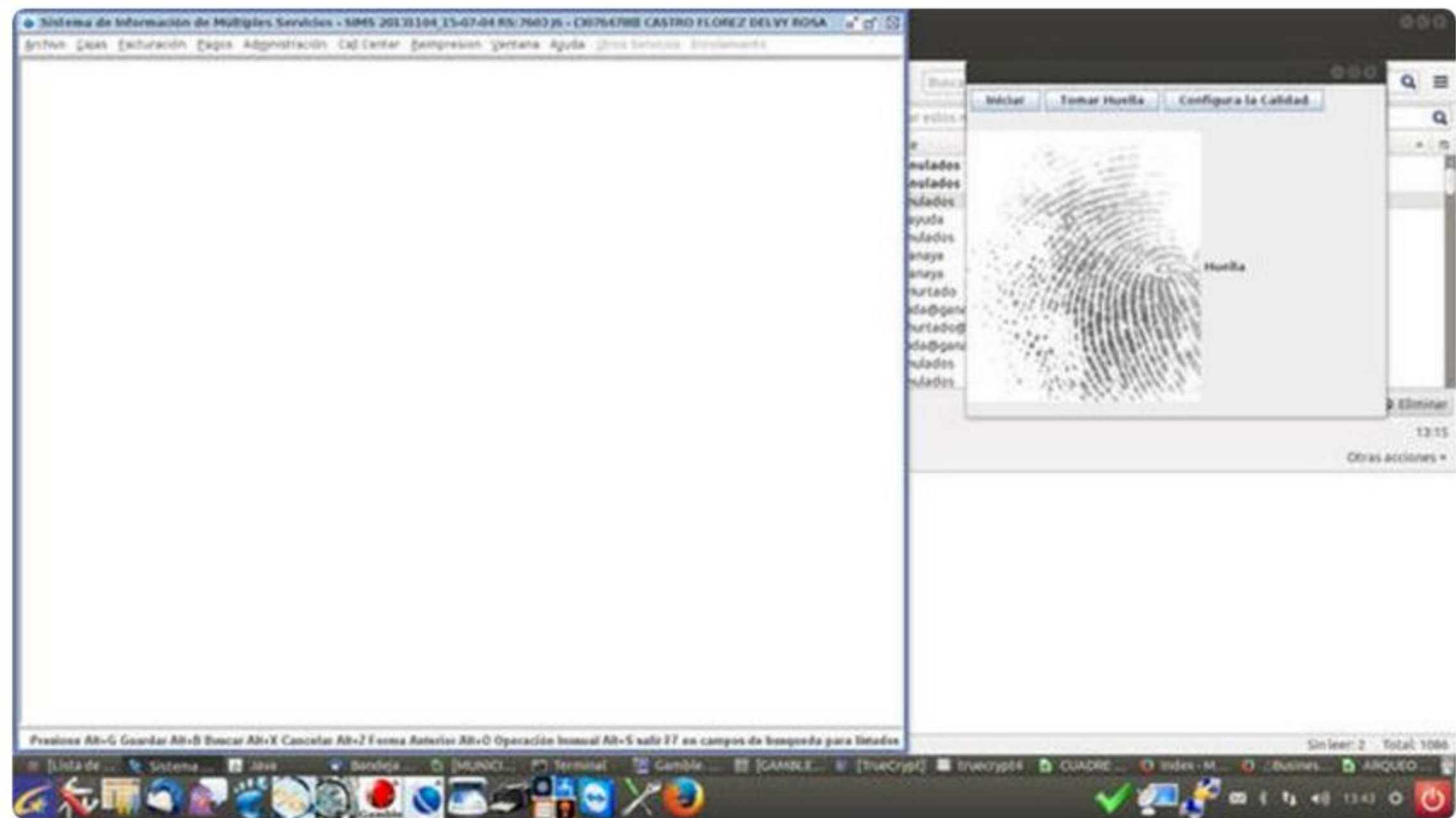


Fingerprints....



Yonathan Klijnsma
@ydklijnsma

Stealing fingerprints from unauthenticated VNC;
[@shodanhq](#) never ceases to amaze me :)
shodan.io/host/190.255.2...




Swatting 2.0....

The screenshot shows a mobile web application interface for Atascocita, Texas. The browser title is "Inform Mobile - [FormHTMLQuery]". The navigation bar includes "Login/Logout", "Queries", "Messages", "Drafts", "Units", "Calls", "Status", "Tools", "Options", and "Help". The status bar shows "Call:" and "Status: LOGGED OUT". The main content area features the Atascocita logo and a "Login" button. Below the logo, there is a "Unit ID:" dropdown menu set to "E29". Underneath, there are two columns: "Unselected" and "Selected". The "Unselected" column lists crew members: Adelman, Matt; Bezdek, Ernest; Botsford, William; and Boyles, Bill. There are arrows below each column to move members between them. At the bottom of the screen, the address "505 WILDWOOD FOREST DR|BUDDE RD" is visible, along with "Clear Route" and "Recalculate" buttons. The Windows taskbar at the bottom shows the time as 3:57 AM on 1/17/2016.



Medical devices

 **Yonathan Klijsma**
@ydklijsma

And there you have it, a machine controlling an X-Ray device on VNC with patient data open..
shodan.io/host/189.70.24...



Some notes on publishing these screenshots.

Some people complain to Dan, Shodan or Me about some of the screenshots. Let me explain some of the data I published in talks or Twitter:

- The severe items (f.e medical devices or power control) are already fixed
- Some of the data I post on Twitter is in fact more than a year old, because it took a long time to fix
- There is tons more than I actually publish or Tweet, its too problematic to expose or contains way too sensitive data



Some notes on publishing these screenshots.

I usually cooperate with ICS-CERT or direct vendors / organisations for the things I find that are serious.

I used to send out bulk data but it was quite unworkable for most so I filter out most of the data before sending it. I do this in my spare time.



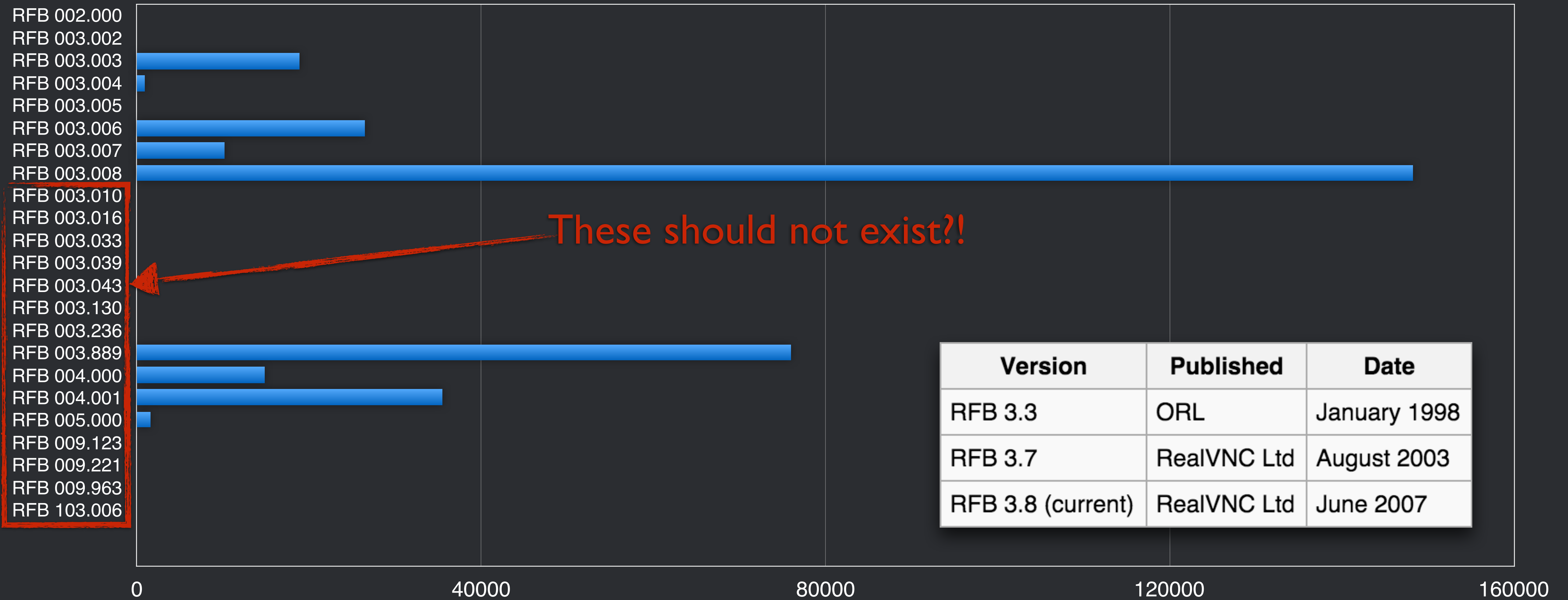
Lets look at some statistics for VNC

I 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.

The numbers are higher than my last talk, due to better scan results and actually more devices coming online!



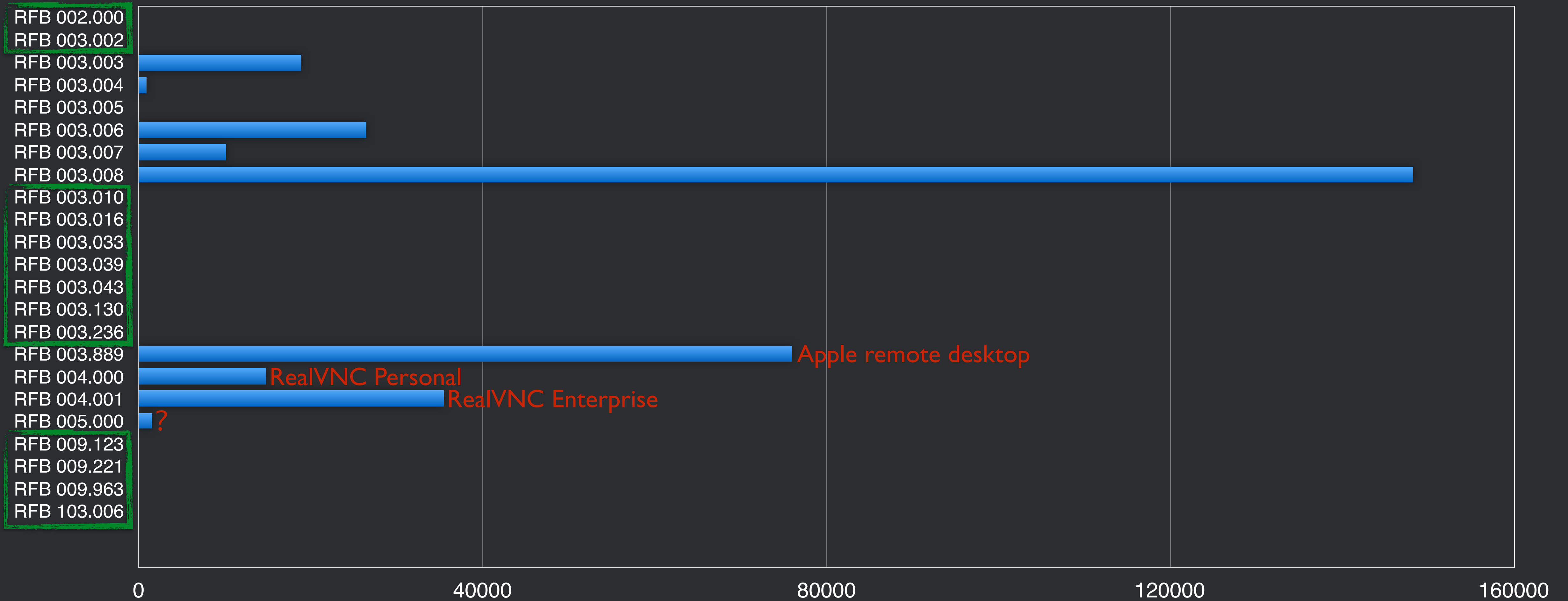
Lets look at some statistics for VNC



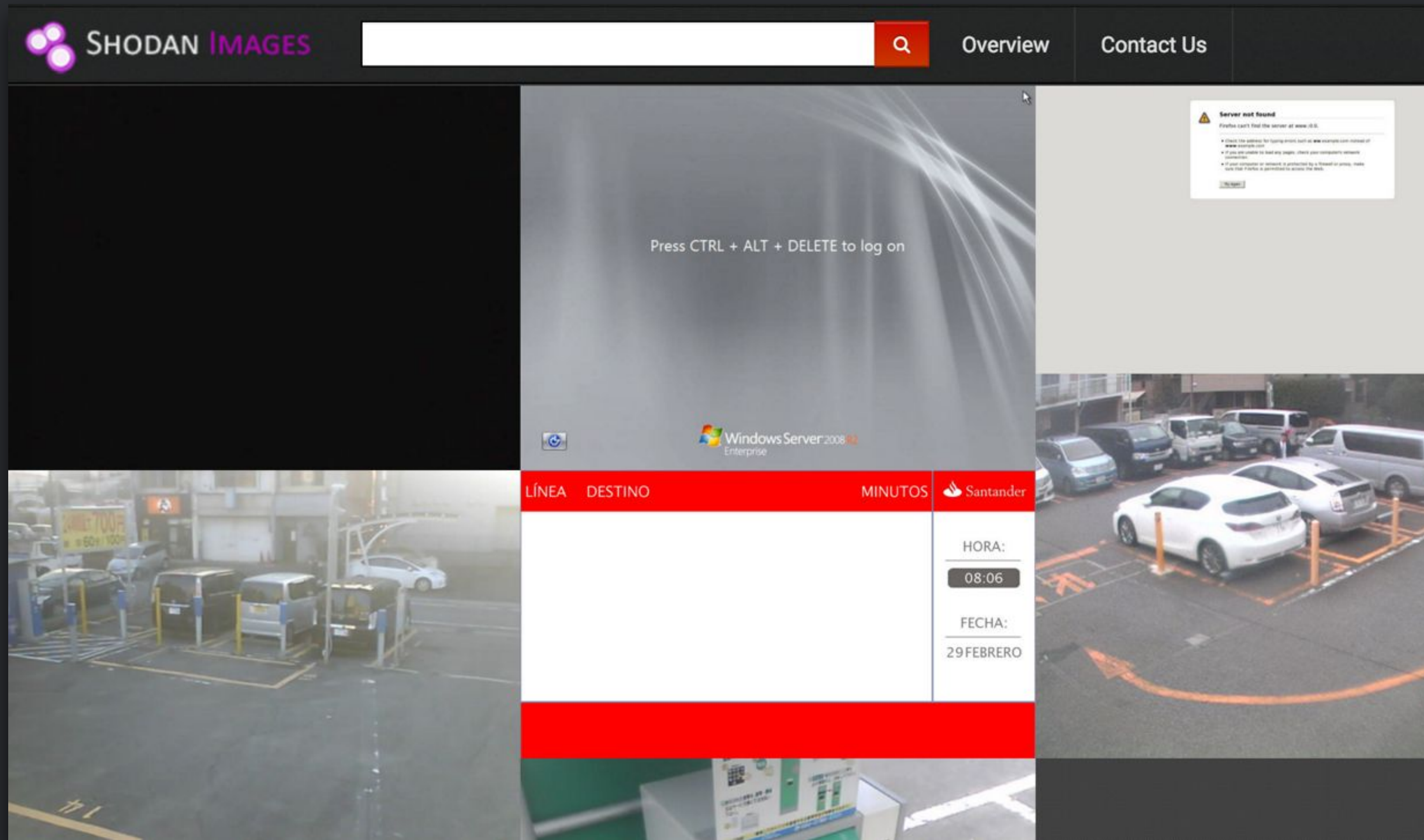
Version	Published	Date
RFB 3.3	ORL	January 1998
RFB 3.7	RealVNC Ltd	August 2003
RFB 3.8 (current)	RealVNC Ltd	June 2007



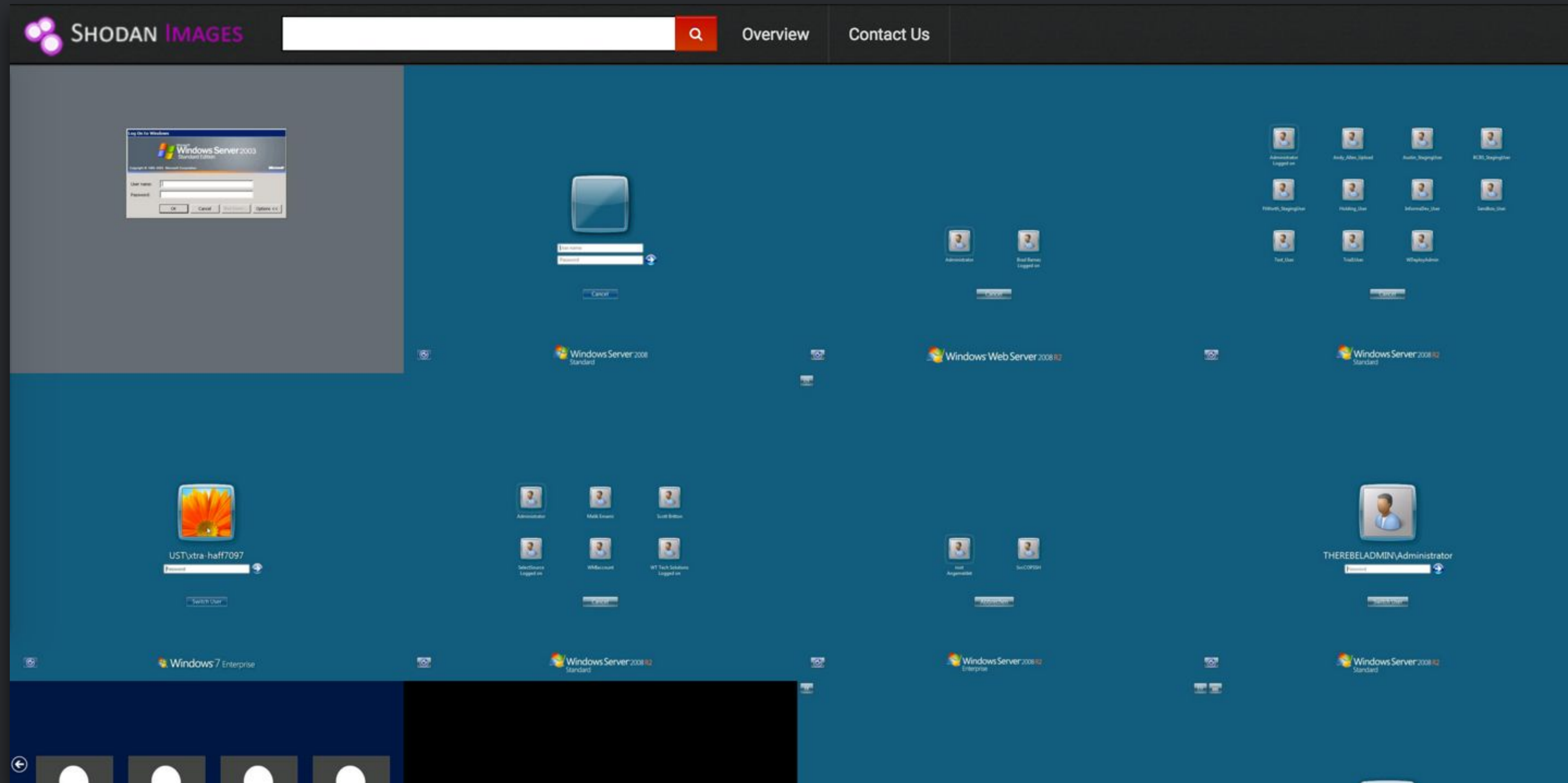
Lets look at some statistics for VNC



images.shodan.io



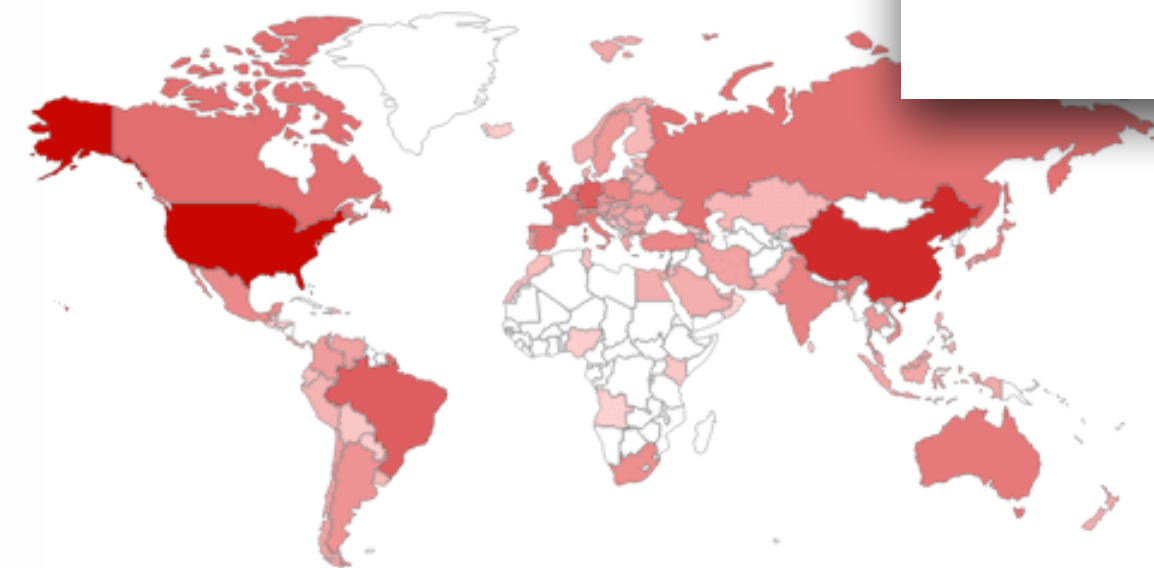
images.shodan.io - RDP



images.shodan.io - RDP

Total results: 3,680,165

TOP COUNTRIES



United States	1,099,932
China	587,909
Germany	161,157
Brazil	158,022
United Kingdom	109,379

TOP ORGANIZATIONS

Amazon.com	197,430
Hangzhou Alibaba Advertisi...	130,931
Microsoft Azure	102,155
Aliyun Computing Co., LTD	68,447
Deutsche Telekom AG	51,594

Added on 2016-04-15 08:43:00 GMT

 United States, Boydton

[Details](#)

Issued By:

|- Common Name: **zcol11**

Issued To:

|- Common Name: **zcol11**

Supported SSL Versions

TLSv1


Remote Desktop Protocol

\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

1.217.51.50

BORANET

Added on 2016-04-15 08:43:00 GMT

 Korea, Republic of, Seoul

[Details](#)

Remote Desktop Protocol

\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

187.105.25.205

bb6919cd.virtua.com.br

NET Virtua

Added on 2016-04-15 08:43:00 GMT

 Brazil, Rio De Janeiro

[Details](#)

Remote Desktop Protocol

\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00



images.shodan.io - RDP

Carver Technologies - Usage notice

Carver Technologies - Usage notice

NOTICE TO USERS

THIS IS A PRIVATE COMPUTER SYSTEM. It is for authorized use only.

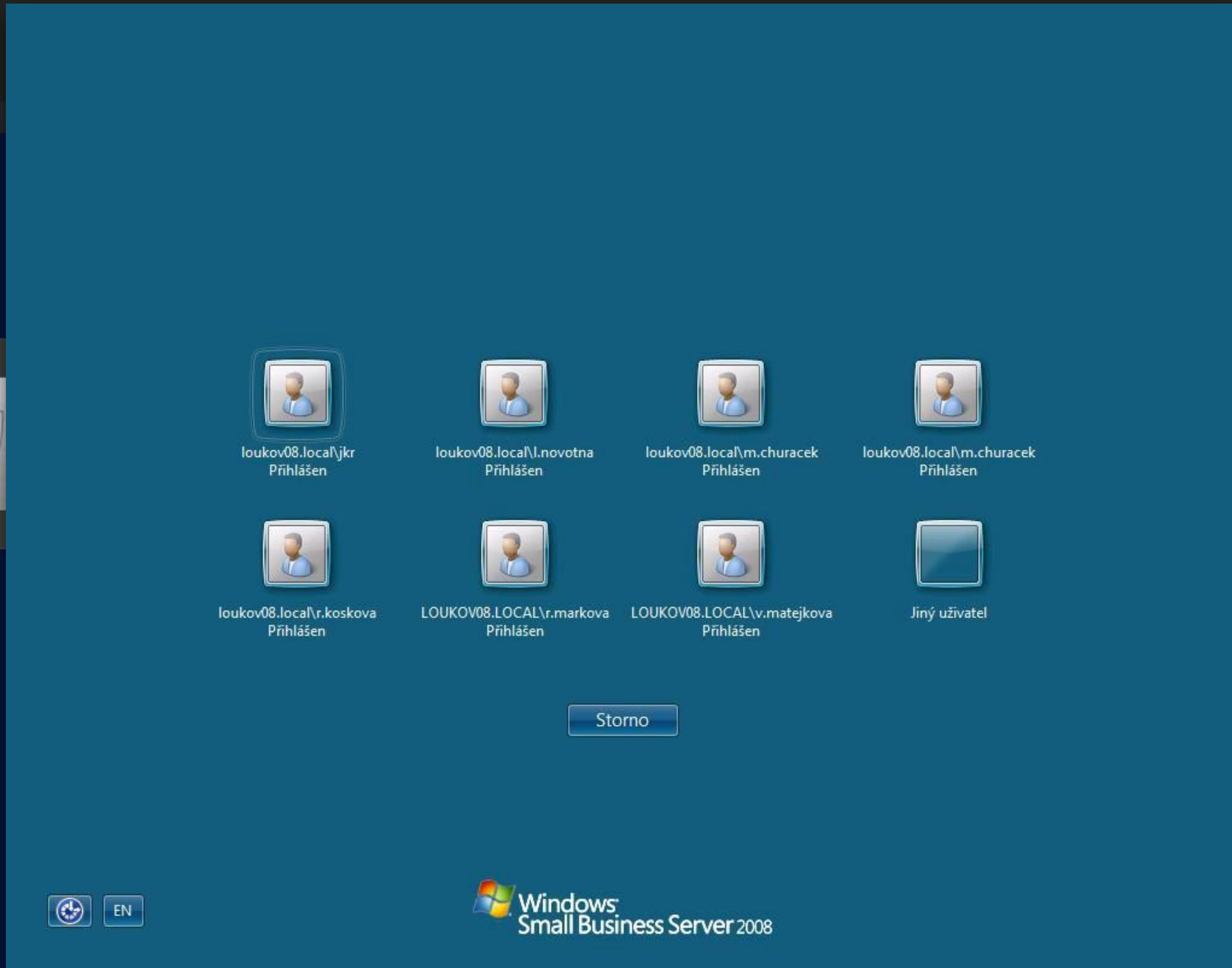
Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site personnel.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties.

By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.



images.shodan.io - RDP



HoneyVNC

With all of the scans I do I couldn't find any proper honeypot that would allow actual interaction. Most of the half-working honeypots support the authentication step but that's about it, no visual data or anything.

I decided to make one, because I like VNC and was wondering who was also poking these devices besides Dan, Shodan and Me.



HoneyVNC

I implemented a 'full interaction' VNC honeypot I've named 'HoneyVNC'. It is still under development but currently features:

- Password authentication on/off (allows you to see brute force attempts)
- Visuals (Actual screen data is being send over to give the impression of a real device on the other end)
- Input can be used to browse around the fake virtual appliance behind the VNC server.
- Sessions are logged for every time a successfully negotiated connection is seen. Everything is logged with a replay-able timestamped file format (mouse and keyboard)



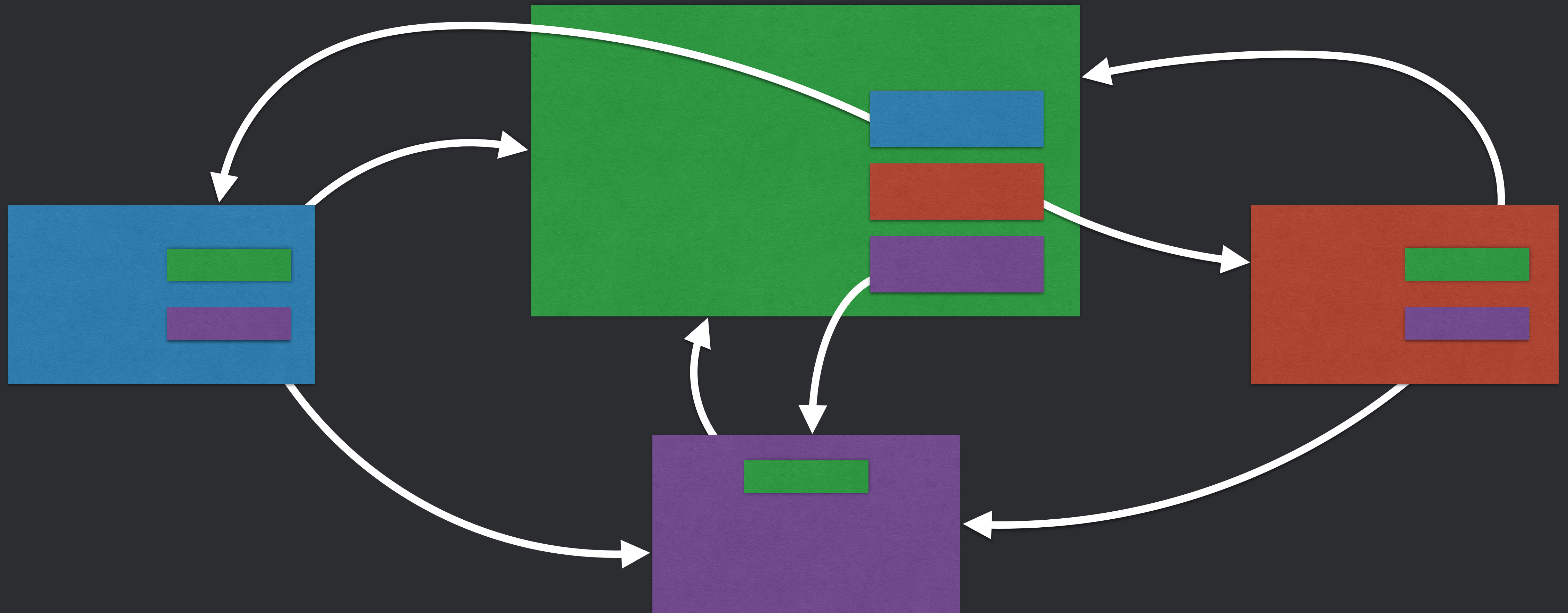
HoneyVNC

There are items I'm still working on to incorporate properly:

- A web application to replay the session logfiles with actual visual representation of what happened in a session.
- Virtual environment design: A honeypot owner can design its own virtual appliance behind the honeypot.



HoneyVNC - Virtual appliances



HoneyVNC

Why not run an actual VNC server:

- Annoying to setup and secure properly, you have to think about all the routes the attacker could go
- HoneyVNC is just a consolidated Python program, there's no jail to break out of because it doesn't have one
- Its Python, runs pretty much anywhere which makes HoneyVNC very portable



HoneyVNC - Findings

I ran a basic version (you could login and get a random screen with uninitialised memory) for about 3 months on a couple different environments.

I had some interesting (unexpected) results.



HoneyVNC - Findings

- Targeted scanning
 - Scans that hit my residential uplinks didn't pass by at data center
 - Known webhosting ranges were not scanned



HoneyVNC - Findings

- **Bruteforcing**
 - When I presented no authentication some would still attempt logins
 - Some were using lists (although I didn't have proper logging)



HoneyVNC - Findings

- **Lots of automated interaction**
 - Even though I presented garbage in the screen buffer there was automated keyboard input. Most of the input contained sentences similar to:
 - del / rm variants
 - echo “r00ted by <insert some lame nickname>”



HoneyVNC - Findings

- **Some manual interaction:**
 - There were some manual interaction moments. Mostly people not understanding the garbage and just randomly clicking and moving (probably thinking to 'refresh' the screen to get a proper image), the classic "if I click faster and harder it will respond" pattern
 - When I was (finally) able to present a screenshot I stole from another VNC appliance someone really wanted to see settings.



HoneyVNC - Can I have/run it?!

It is not ready for a public release yet, there's issues to work out and features to implement still. I want to deliver and as-easy-to-use-as-possible honeypot with good (and meaningful) log results.

I've had to implement the RFB protocol by hand, which sucks. I like VNC but I don't like the protocol... at all.... it. is. a. pain.

As soon as I feel its actually usable for other people I will make it public on Github so other people can play around with it.



HoneyVNC - Development timeline

- **First version (August 2015):** single Python file with a fixed statemachine
- **Second version (October 2015):** Tried making a hacky RFB implementation
- **Third version (current):** found the awesome libvnc and currently making Python bindings. The idea is to have precompiled libvnc binaries and a separate HoneyVNC script with configuration.

Can't run the current version (completely overhauled)... :(sorry no demo.



RFB logging in Bro!

At my company (Fox-IT) we've implemented the RFB protocol in Bro. It features the full protocol and logs the start of sessions and the end (so you can get actual sessions worked out over the network). It currently logs:

- Source / Destination
- Client & server versioning (minor & major)
- Authentication method
- Which auth was used (based on auth list)
- Session sharing flag
- Desktop name
- Width and Height



RFB logging in Bro!

Committed last Wednesday:

- <https://github.com/bro/bro/commit/9d0899325a6a4391764cc541f4c41b4353ff79e6>
- <https://goo.gl/6G5Aun>



RFB logging in Bro!

To come, a Bro policy to dump screenshots from live VNC sessions.





Thanks for your time & attention, lets get back to our fires :(

