RSAConference2018
San Francisco | April 16–20 | Moscone Center


SESSION ID: SBX1-W2

# ROBOTIC TELEPRESENCE – IS YOUR ENEMY WATCHING YOU?

**Dan Regalado**

Security Researcher
Zingbox Inc
@danuxx

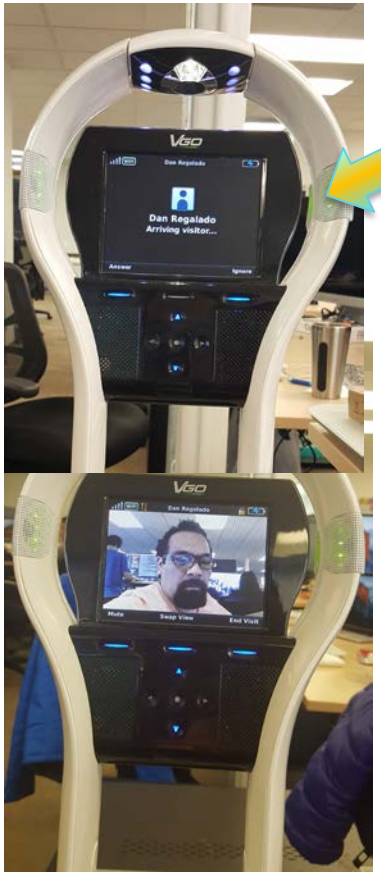

# WHEN YOU HEAR ABOUT ROBOTIC TELEPRESENCE

# WHAT IS THE FIRST THING THAT COMES TO YOUR MIND?

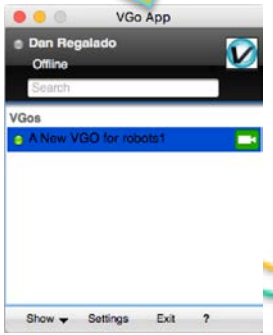
# Expectation

# Reality

# How it works?




VGoNet
Cloud Network


# Use Cases


## THE BENEFITS ARE GREAT, NO DOUBT

## DO YOU SEE ANY SECURITY CONCERNS?

# What if someone else is watching you?


# BREAKING INTO THE ROBOT

# Responsible Disclosure

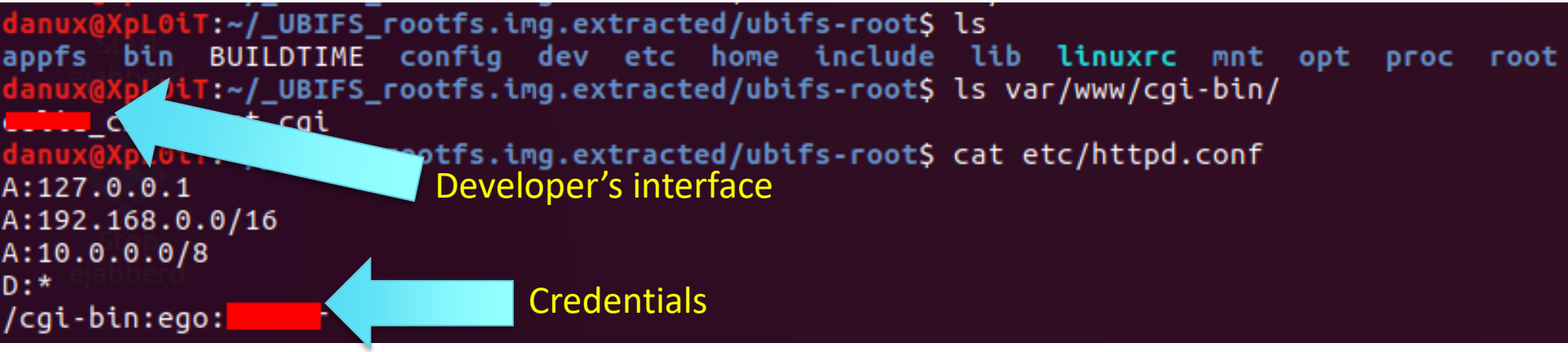

- All the vulnerabilities identified were reported to vendor via ICS-CERT
- A total of three CVEs were issued
  - ✓ CVE-2018-8858: Insufficiently Protected Credentials
  - ✓ CVE-2018-8860: Cleartext Transmission of Sensitive Information
  - ✓ CVE-2018-8866: Improper Neutralization of Special Elements (RCE)
- At this moment, the patch has not been released

# Intercepting Firmware Update



| | | | | | | |
|---|---|---|---|---|---|---|
| 192.168.10.131 | 75.101.136.21 | HTTP | 356 | GET | [redacted] | v1/vgo/release/build-[redacted].releases_3.0.1. |
| 75.101.136.21 | 192.168.10.131 | HTTP | 126 | HTTP | [redacted] | ation/octet-stream) |
| 192.168.10.131 | 75.101.136.21 | HTTP | 364 | GET | [redacted] | v1/vgo/release/build-[redacted].releases_3.0.1. |
| 75.101.136.21 | 192.168.10.131 | HTTP | 831 | HTTP | [redacted] | ation/octet-stream) |
| 192.168.10.131 | 75.101.136.21 | HTTP | 358 | GET | [redacted] | v1/vgo/release/build-[redacted].releases_3.0.1. |
| 75.101.136.21 | 192.168.10.131 | HTTP | 629 | HTTP | [redacted] | ation/octet-stream) |
| 192.168.10.131 | 75.101.136.21 | HTTP | 356 | GET | [redacted] | v1/vgo/release/build-[redacted].releases_3.0.1. |
| 75.101.136.21 | 192.168.10.131 | HTTP | 351 | HTTP | [redacted] | ation/octet-stream) |
| 192.168.10.131 | 75.101.136.21 | HTTP | 360 | GET | [redacted] | v1/vgo/release/build-[redacted].releases_3.0.1. |
| 75.101.136.21 | 192.168.10.131 | HTTP | 1207 | HTTP | [redacted] | ation/octet-stream) |
| 192.168.10.131 | 75.101.136.21 | HTTP | 352 | GET | [redacted] | v1/vgo/release/build-[redacted].releases_3.0.1. |
| 75.101.136.21 | 192.168.10.131 | HTTP | 324 | HTTP | [redacted] | lain) |
| 192.168.10.131 | 75.101.136.21 | HTTP | 360 | GET | [redacted] | v1/vgo/release/build-[redacted].releases_3.0.1. |
| 75.101.136.21 | 192.168.10.131 | HTTP | 647 | HTTP | [redacted] | ation/octet-stream) |
| 192.168.10.131 | 75.101.136.21 | HTTP | 340 | GET | [redacted] | v1/vgo/release/build-[redacted].releases_3.0.1. |
| 75.101.136.21 | 192.168.10.131 | HTTP | 288 | HTTP | [redacted] | lain) |
| 192.168.10.131 | 75.101.136.21 | HTTP | 350 | GET | [redacted] | v1/vgo/release/build-[redacted].releases_3.0.1. |
| 192.168.10.131 | 75.101.136.21 | HTTP | 349 | GET | [redacted] | v1/vgo/release/build-[redacted].releases_3.0.1. |
| 192.168.10.131 | 75.101.136.21 | HTTP | 373 | GET | [redacted] | v1/vgo/release/build-[redacted].releases_3.0.1. |

# Accessing the Firmware



# Accessing Developer's Interface



[redacted] Developer Page

**North End Technologies, Inc.**

Choose which command you want to run

- ○ Change [redacted]'s identity
  - [redacted] account name [redacted]-70[redacted]
  - [redacted] password [redacted]
  - XMPP server vgocom.com
- ○ Change Celia Update Track : Update Track release
- ○ poweroff
- ○ reboot
- ○ App restart
- ○ uname -a
- ○ netstat -a
- ○ dmesg
- ○ ls folder /appfs/opt/egocom
- ○ process list (ps)
- ○ cpu (top)
- ○ view log (warning, slow!)

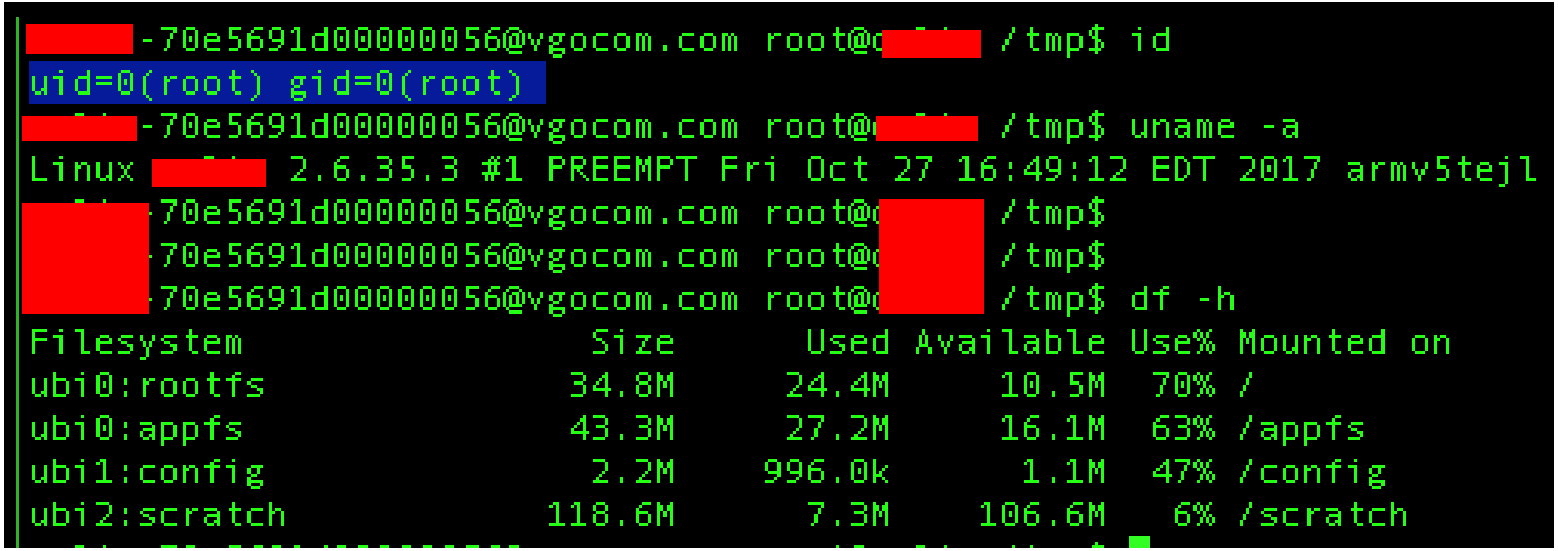
Submit

192.168.10.191/cgi-bi

**Running processes:**

```
PID  Uid        VSZ Stat Command
  1 root      3076 SW   init
  2 root           SW   [kthreadd]
  3 root           SW   [ksoftirqd/0]
  4 root           SW   [watchdog/0]
  5 root           SW   [events/0]
  6 root           SW   [khelper]
  9 root           SW   [async/mgr]
 34 root           SW   [events/0]
 35 root           SW   [events_long/0]
 36 root           SW   [events_nrt]
132 root           SW   [sync_supers]
134 root           SW   [bdi-default]
136 root           SW   [kblockd/0]
146 root           SW   [khubd]
149 root           SW   [kseriod]
161 root           SW   [cfg80211]
173 root           SW   [rpciod/0]
182 root           SW   [khungtaskd]
183 root           SW   [kswapd0]
184 root           SW   [aio/0]
185 root           SW   [nfsiod]
186 root           SW   [crypto/0]
334 root           SW   [mtdblock0]
339 root           SW   [mtdblock1]
344 root           SW   [mtdblock2]
349 root           SW   [mtdblock3]
354 root           SW   [mtdblock4]
359 root           SW   [mtdblock5]
364 root           SW   [mtdblock6]
369 root           SW   [mtdblock7]
374 root           SW   [mtdblock8]
383 root           SW   [ubi_bgt0d]
384 root           SW   [ubiblk6]
387 root           SW   [ubiblk6]
432 root           SW   [hwevent]
433 root           SW   [vgo_security]
```

# Shell Injection and Root Access

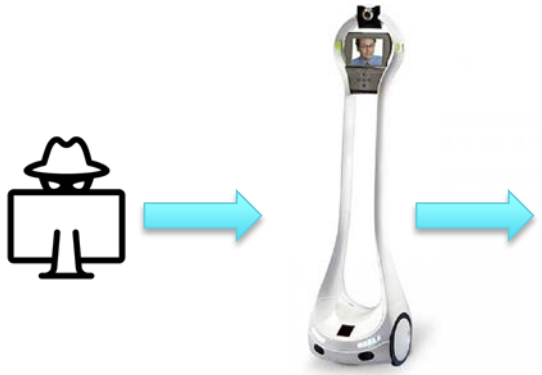



# GOT R00T, SO…
# GAME OVER?

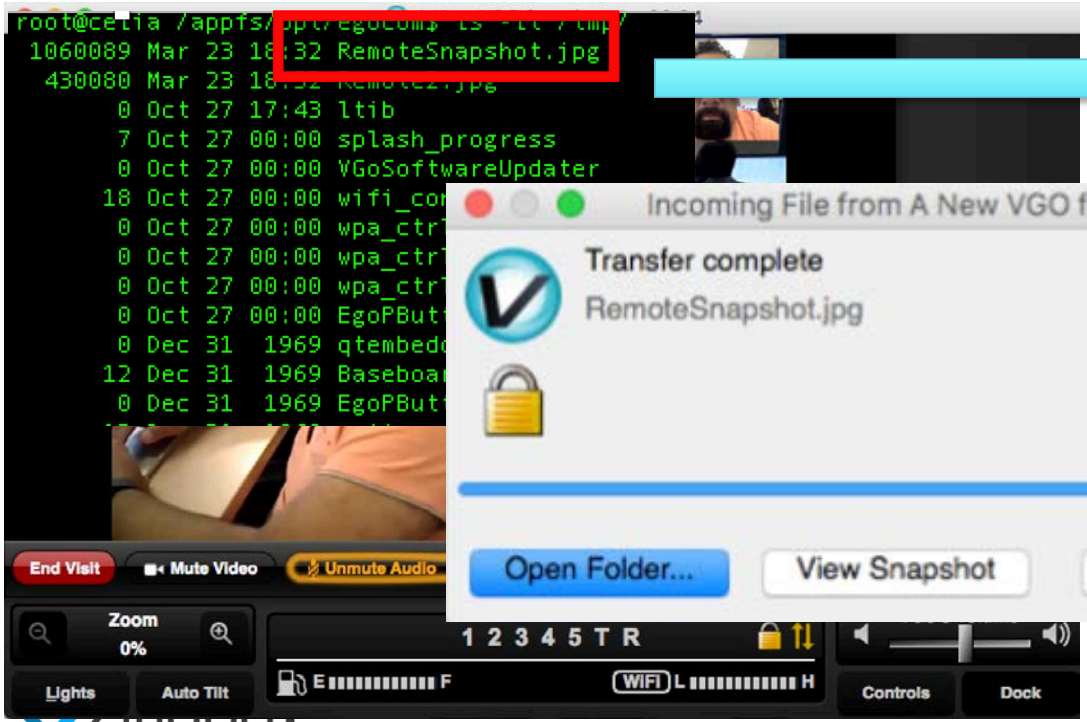
# Stealing WiFi Credentials

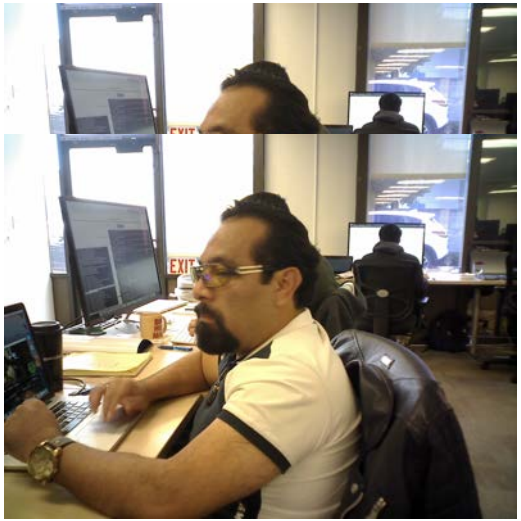


```
ctrl_interface=/var/run/wpa_supplicant
update_config=1

network={
        ssid="ZingMi[redacted]"
        psk="[redacted]"
        proto=RSN
        key_mgmt=WPA-PSK
        pairwise=CCMP
        group=CCMP
        disabled=1
}

network={
        ssid="IPhone 0SX 7.0"
        psk="[redacted]"
        proto=RSN
        key_mgmt=WPA-PSK
        pairwise=CCMP
        group=CCMP
        disabled=1
}
```



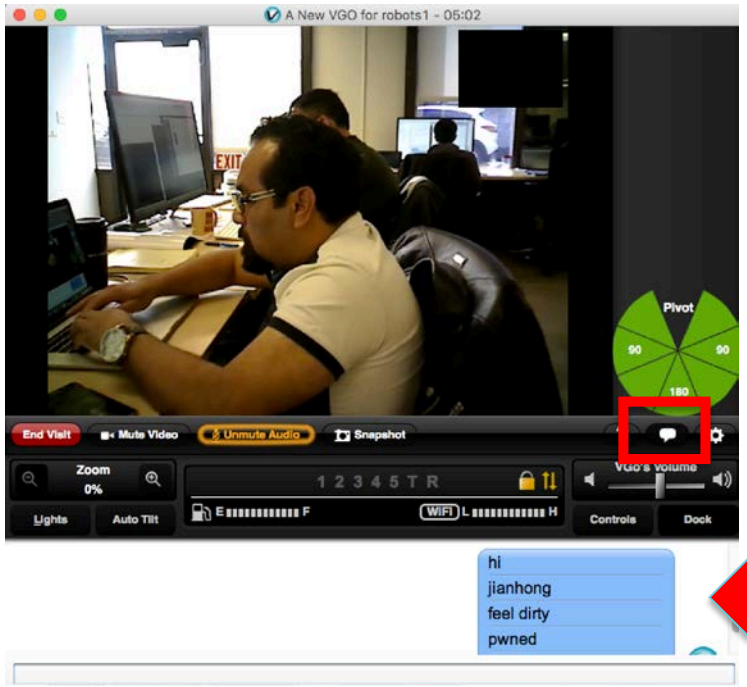
# Stealing Pictures taken

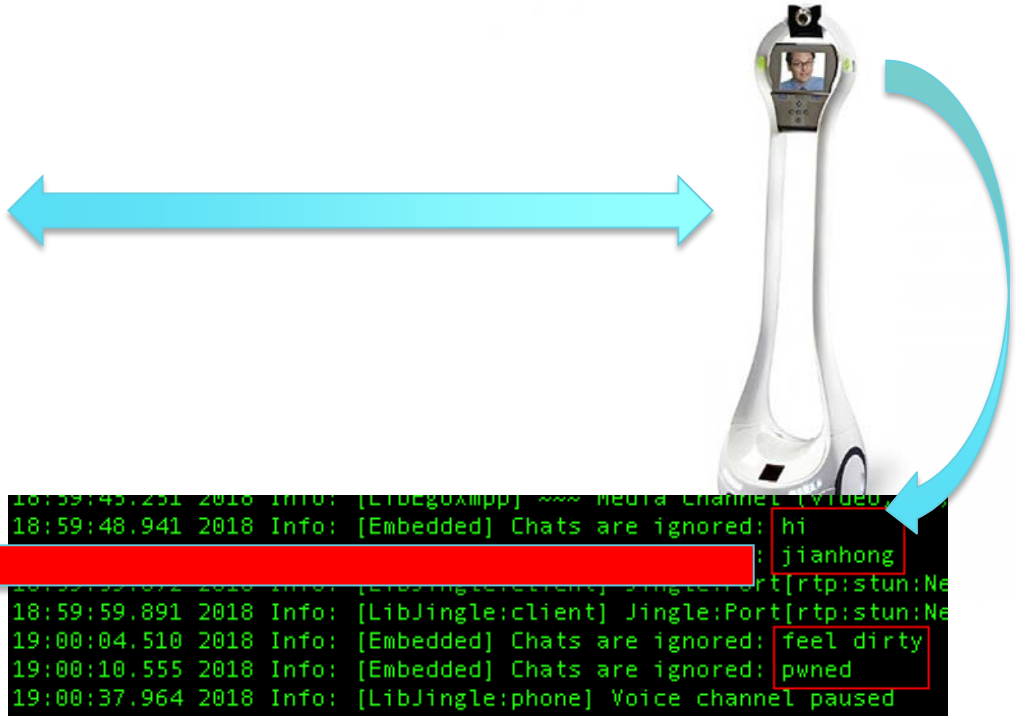



# DEMO

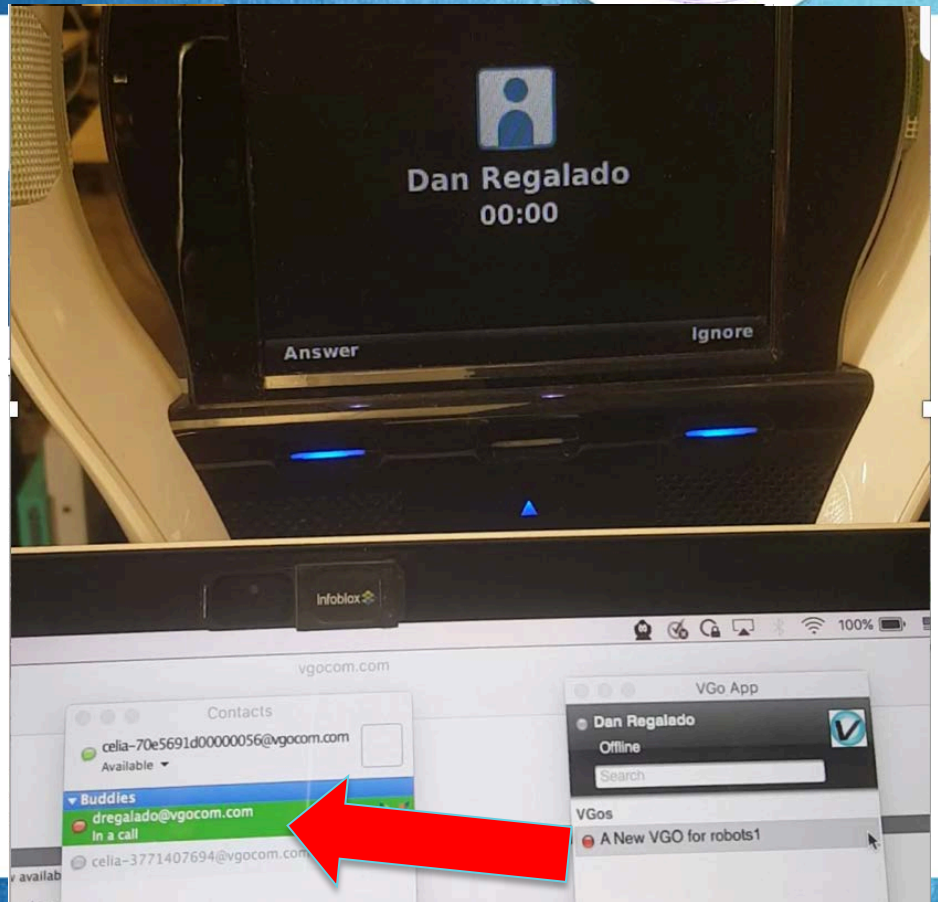
# Sniffing Chat Conversations



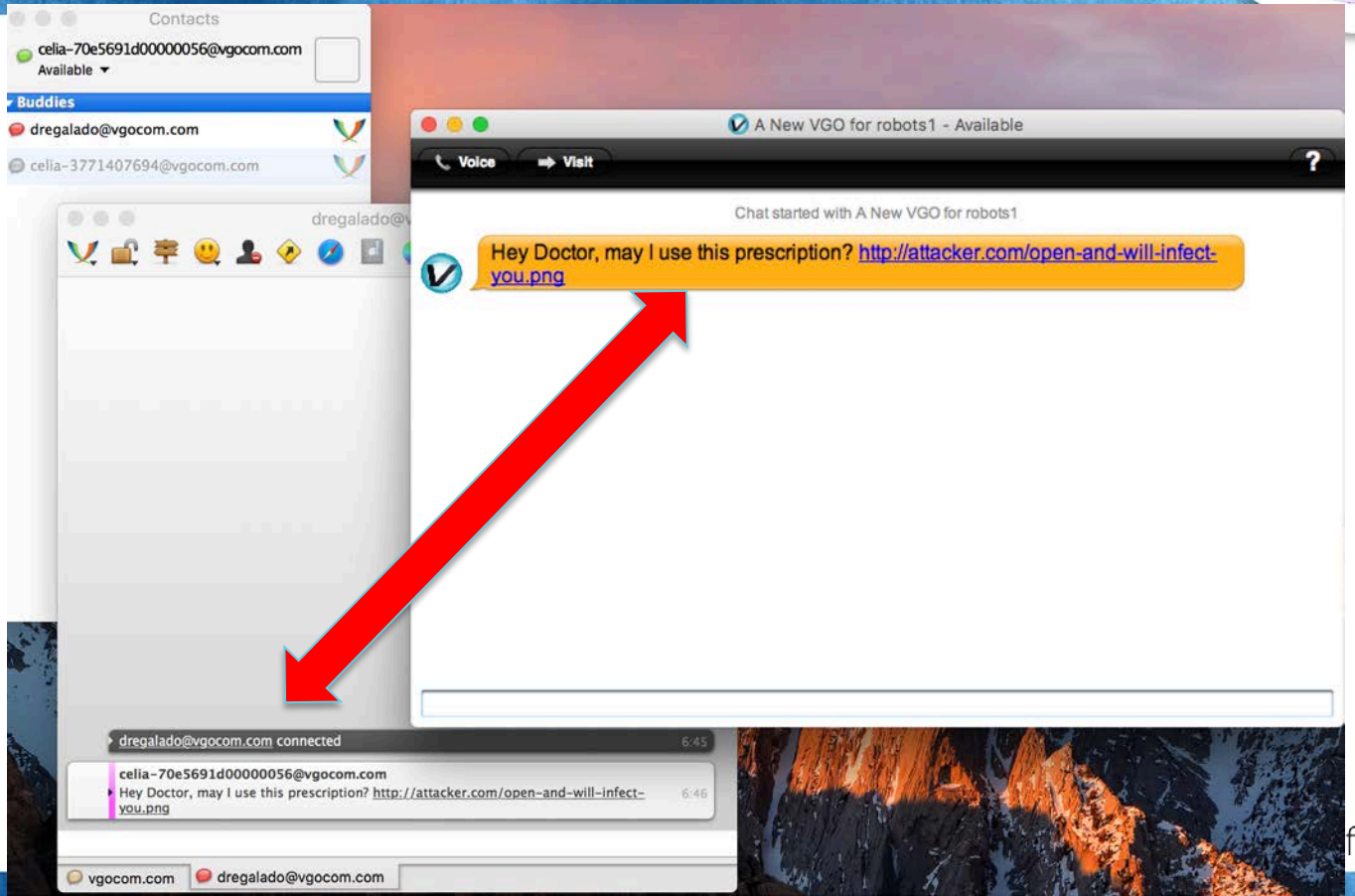
# Monitoring Doctor Calls




Zingbox

# First ever Robot Social Engineering



# Takeaways


- Manufacturers: Add security code review/PenTest into Software Dev Cycle
- Manufacturers: Secure Firmware Updates
- Manufacturers: Remove Developer interfaces in Production
- Customers: Ask manufacturers to show evidence of security assessments

# Summary



- Robotic Telepresence is great technology making life easier
- We just need to invite security to the party
- We cannot do background check on the Robot
  - Better to make sure it is trustworthy by hacking it proactively ☺
- IoT is the door to new technologies
  - But we do not want it to be the door into our Privacy

Thanks!
Any questions?

**@danuxx**