DEFCON 24

Light Weight Protocol!
Serious Equipment!
Critical Implications!

—·–=[Lucas Lundgren]=–·—

@acidgen

Senior Security Consultant

FortConsult

a part of

NCC GROUP

· · ·——— ■ Login to see presentation ■ ———· · ·

Username:_

Password:

WHOAMI

king zypzyp ftw

--ans/
trasher

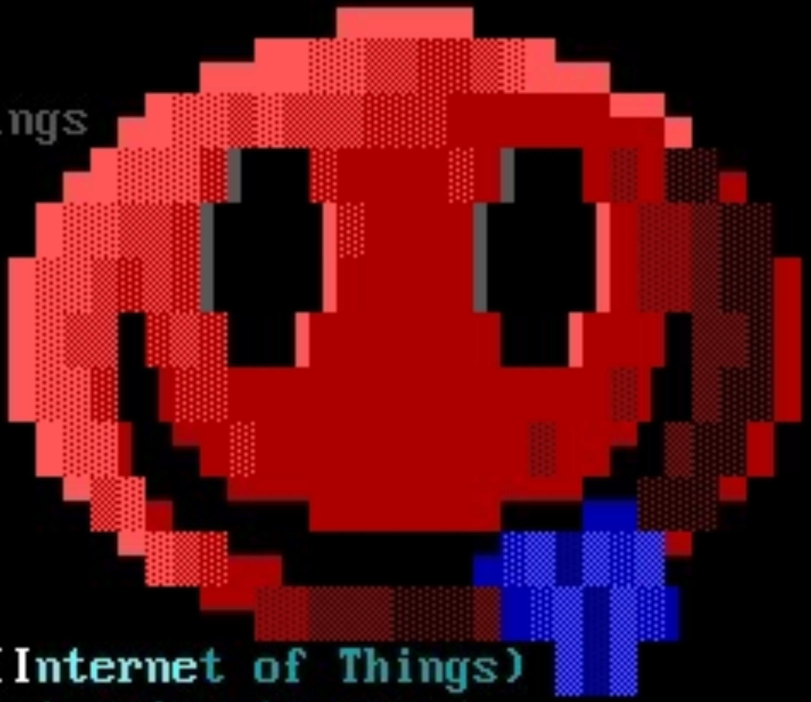
Lucas Lundgren
ACiDGEN

- Been breaking stuff since I was 12 (First reported vuln)
- Worked for companies such as Sony Ericsson and IOActive (to name a few)
- Been a part of the super awesomesauce Corelan Team - !mona ftw
- Spent time in alot of "unhackable" environments and 'puters
- I Do fuzzing, exploit dev, webapp pwnage, and network pentests
- IoT is someting that always interested me, consumer stuff!

#defcon props to Corelanc0d3r (PVE)

IoT

----Internet of Things



I am going to talk about IoT (Internet of Things)
And yeah I know, but we are just going to cover
one protocol.

Don't get me wrong, I love hooking stuff up!
Getting everything to work seamless is awesome!

But since I'm in Security; This is a curse

Looking at all the devices I have,
and looking at things customers have,
scares me.

It makes me question, is security REALLY
a part of the process, or just something
vendors tackle when shit hits the fan?
Or is it just a 5 minute Automated Vuln-Check
with <insert favv scanner here>

congratsifyouheardaboutit

MQTT

wtf?

WHAT IS IT?

--- Invented in 1998/1999

--- Created by Andy Stanford-Clark & Arlen Nipper

WHY?

--- They wanted to create a new protocol to combat unreliable satellite networks

--- Key Points: Simple
QoS (Quality of Service)
Bandwith efficient
etc etc

MQTT ?

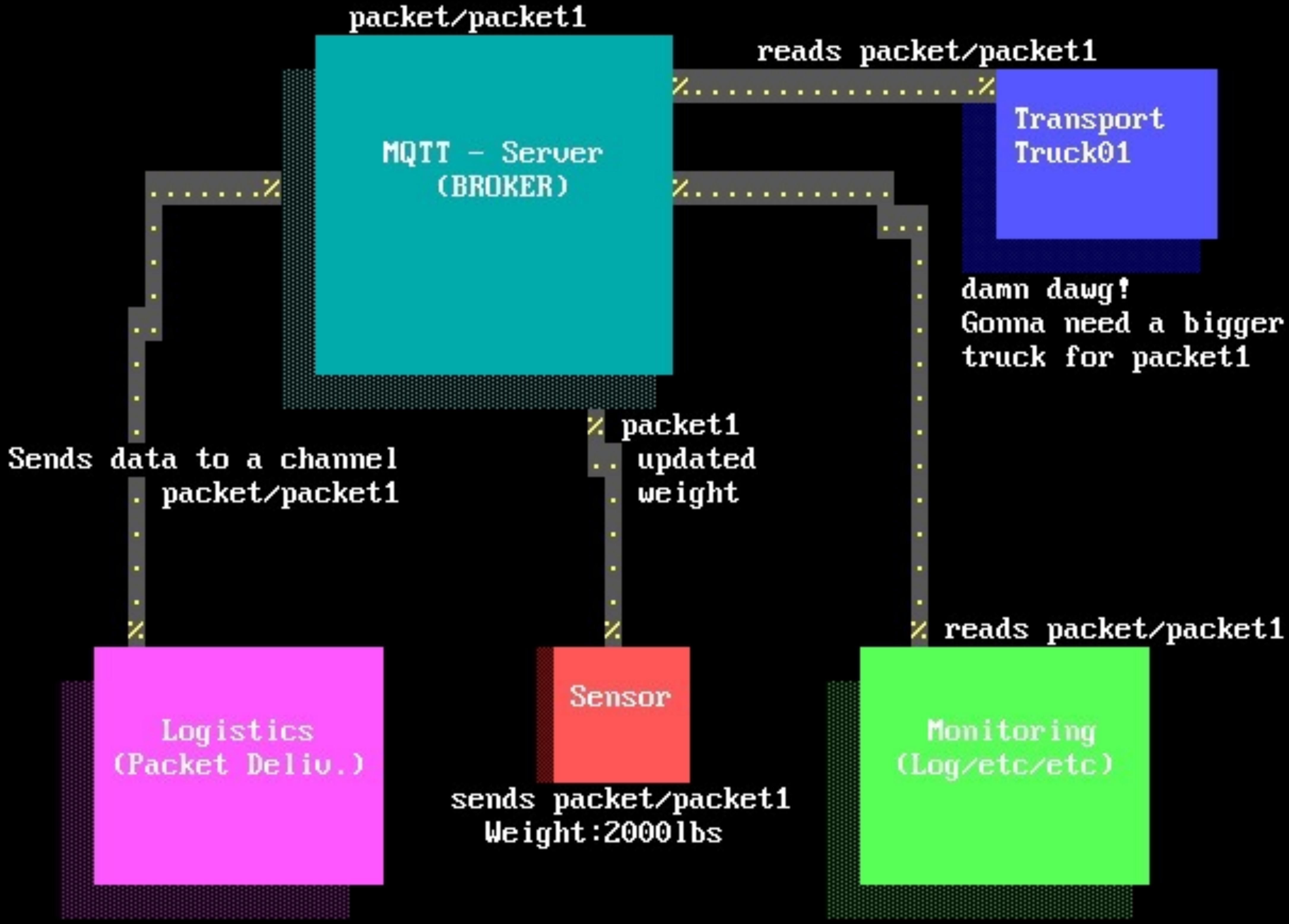
--- Stood for MQ Telemetry Transport
·
·-----Something IBM Something Product

--- Royalty Free as of 2010

--- Officially approved as OASIS Standard Oct 29th 2014

--- Version 3.1.1

01100010 01101111 01110010 01100101 01100100 00111111



packet/packet1

MQTT - Server
(BROKER)

reads packet/packet1

Transport
Truck01

damn dawg!
Gonna need a bigger
truck for packet1

Sends data to a channel
packet/packet1

packet1
updated
weight

reads packet/packet1

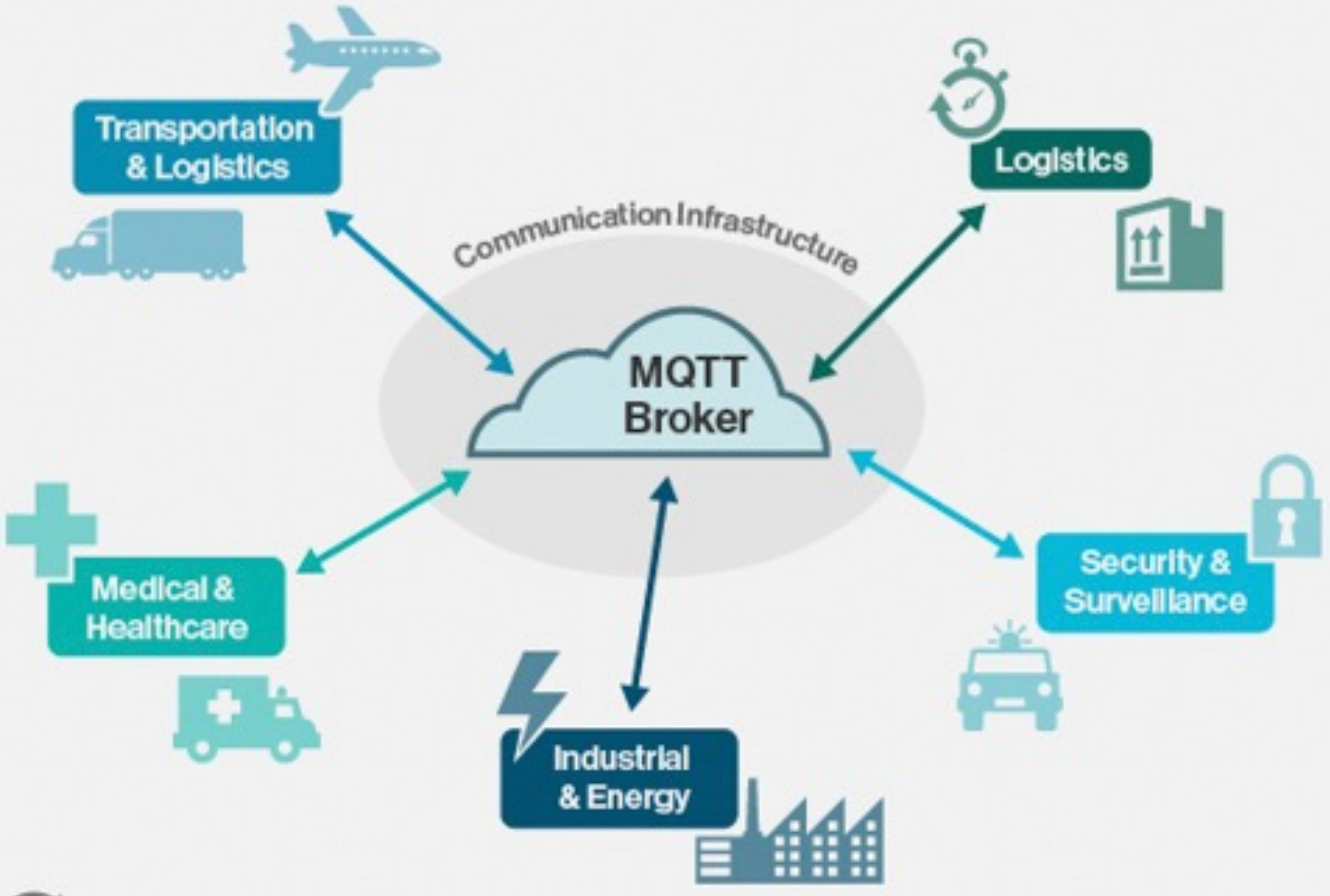
Logistics
(Packet Deliv.)

Sensor

sends packet/packet1
Weight:2000lbs

Monitoring
(Log/etc/etc)

MQTT



TechTarget

TELLME?!

MQTT

MAN!

Did you know?!
Facebook used MQTT for chat
before changing to XMPP...

-"How does the MQTT Work? I Mean what is a broker?
I mean, why? w... Why is the sky blue... Banana!"

- What we know as server, MQTT calls Broker

- Broker - A Person who buys and sells assets for others

- Clients? Clients can both listen and send data to the broker

- Other Clients listen to what is been sent in and reacts

- Depending on how the its set up, the client responds

```
MQTT has channels (Yes almost as IRC)
Example:myhome/attic         <- Here i place every client in the attic
        myhome/attic/sensor1 <- My Temprature sensor in the attic

You can name them ANYTHING: OhLongJohnson/OhDonPiano/whyIeyesYa
                            ^...Seems hard to remember thou
```

Let's move on to the Magic of #

MQTT documentation on the web says not to subscribe to #
SO LETS SUBSCRIBE TO #

SECURITY?

MQTT

RTFM!

According to the manual: There is security...
There are a number of threats that solution providers should consider.

- Devices could be compromised
- Data at rest in Clients and Servers might be accessible
- Protocol behaviors could have side effects (e.g. "timing attacks")
- Denial of Service (DoS) attacks
- Communications could be intercepted, altered, re-routed or Disclosed
- Injection of spoofed Control Packets

MQTT solutions are often deployed in hostile communication environments.

Awww' Cmon man - Internet is a nice place!
above statment is sarcasm

Seems like people didn't bother reading the manual? Que?
http://bit.ly/29an8Iw ◄ Source

#

MQTT

SPLAT

According to some of the vendors, you shall not subscribe to

#

So that is exactly what I did
(Whatch out we got a bad- ass over here)

- Hierarchy with the # sign indicates "EVERYTHING" inside that branch
- # Without any given topics would give us what?
- /something/something/# Shows everything in this topic
- Shodan has some information about it, just the topics

I wanted to scan the entire Internet and extract what ever data there was. Not just the topics...

What Kind of Data can you get?

SHODAN

all your data are belong to us
(port:1883 is the MQTT unencrypted port)

SHODAN.IO

Search Query: port:1883 "MQTT"

Top Countries:
China: 4,921
United States: 3,412
Singapore: 1,312
Japan: 757
Germany: 746

Statistics during time of writing

Total: 17,711

EXAMPLE DATA

Topics:

```
ActiveMQ/Advisory/Consumer/Topic/>
ActiveMQ/Advisory/Connection
ActiveMQ/Advisory/XXXXXXXX/Topic/com/XXXXXXXXX/XXX/XXXXXXXXX/topic
com/XXXXXXXXX/XXX/XXXXXXXXX/topic
ActiveMQ/Advisory/Producer/Topic/com/XXXXXXXXX/XXX/XXXXXXXXX/topic
```

Topics give info, not as much as I want

Data is as accurate as when the shodan scan was done
I BELIVE THERE IS MOAR - LETS SCAN THE INTERNETZ

Props to Shodan.io

#LISTEN

Arnold -"Auugh, Listen to meeaahh..."

Modified some example code on the net
to listen to # on any given server

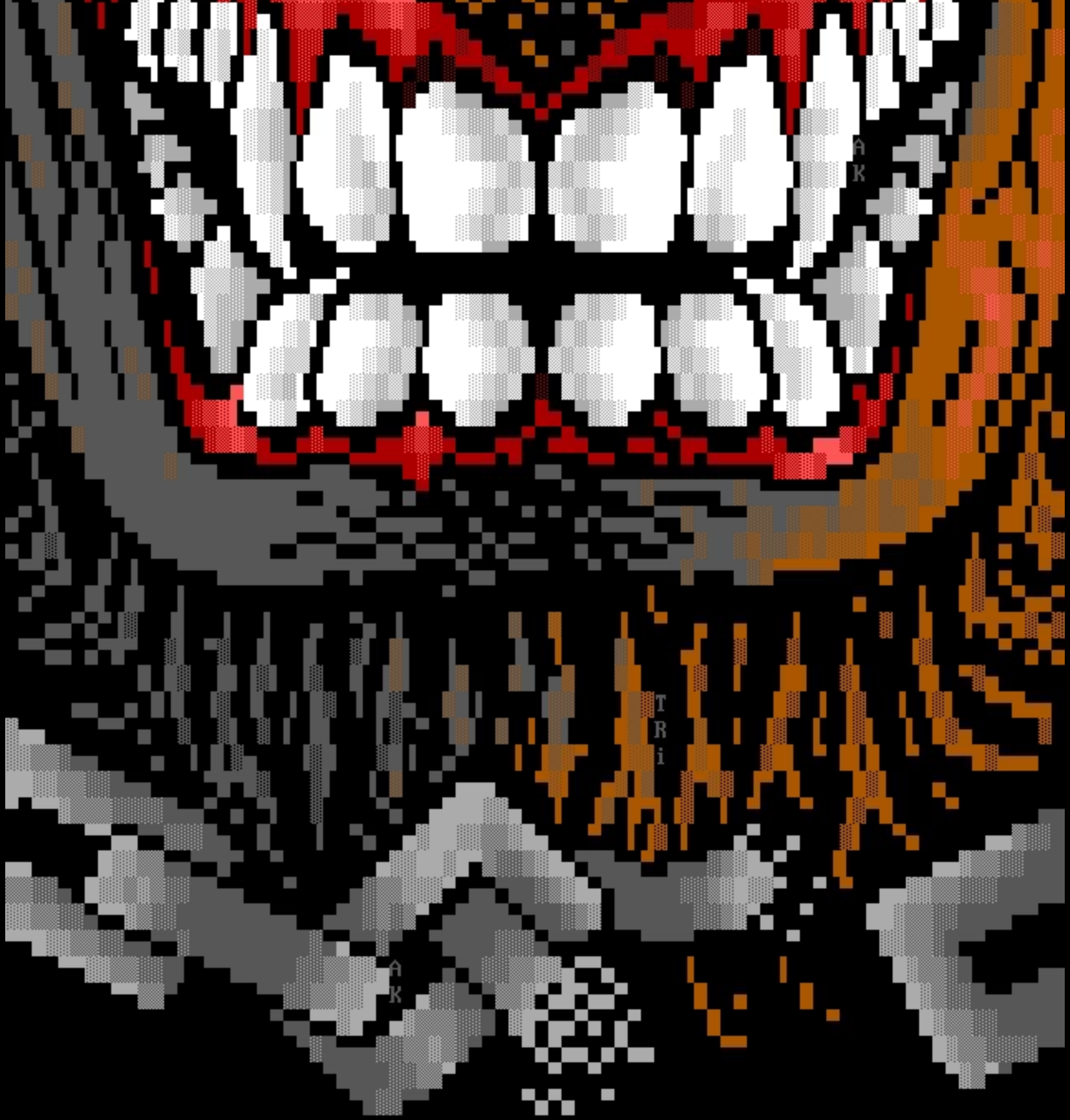
CODE BLOCK

```
require 'rubygems'
require 'mqtt'
#Requires MQTT for Ruby

unless ARGV.length == 1
  puts "Usage: ruby hodor.rb IP"
  puts "Example: ruby hodor.rb 127.0.0.1"
  exit
end

 IP=ARGV[0]

MQTT::Client.connect(IP,1883) do |client|
  client.get('#') do |topic,message|
    puts "#{topic}: #{message}"
  end
end
```

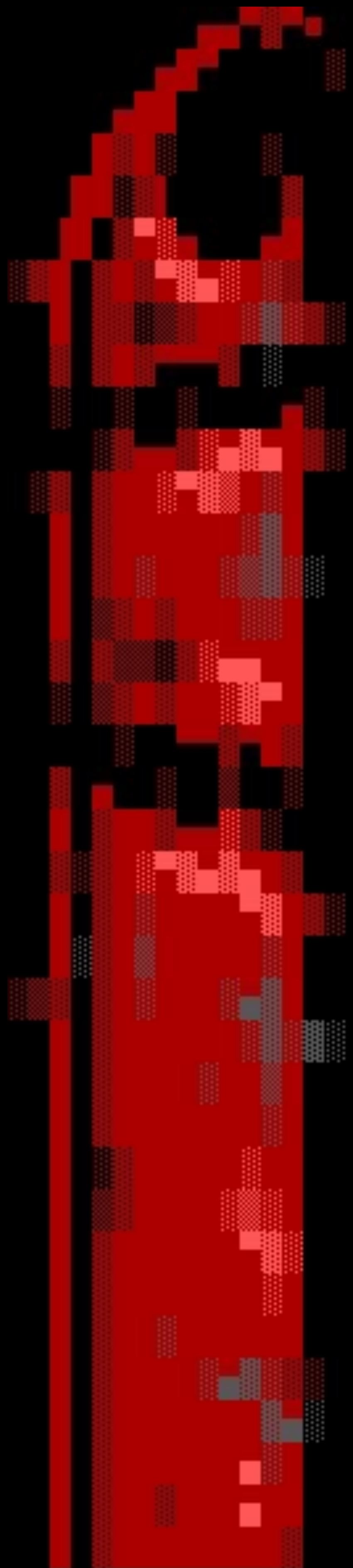


I tried an example server that I found on Shodan, just too see
what kind of data I could find...   Please note that alot data is

CENSURED

```
{"value":{"Id":"231XXXX","User":"14XX","Status":"9","Message":
"Jag är sjukskriven till och med den 12 juni. Jag hänvisar min
telefon till Ett nummer i  XXXXXXås XXXXXXXX 0XX-XXXXXX","From":"2016-XX-XX
vidare"},"sessionId":"77762c24-12c7-4d50-XXXX-XXXXXXXXXXXX"}
```

```
Translate: I'm on a sickleave until the 12th of June
           I forward my calls to a number in XYZ XYZ-AFFILIATE
```



OMFG

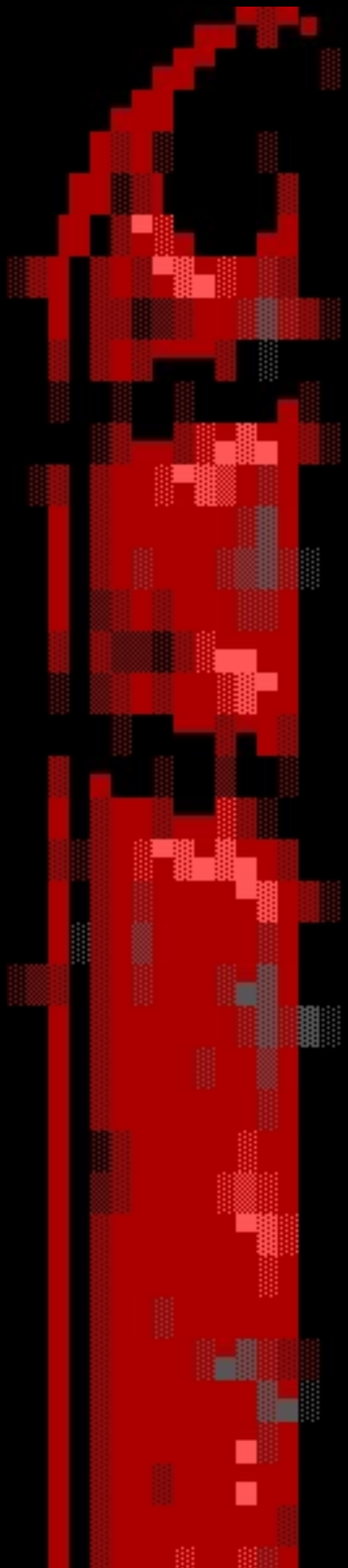
what kind of sorcery is this?!

```
{"value":{"action":"getVoiceMails","argument":null,"_type":
"Request","_id":"0f78a1cb-e9ee-4fdc-b7XX-XXXXXXXXXXXX"},"
sessionId":"0d99bfcd-2e4a-4039-XXXX-XXXXXXXXXXXX"}
ebe9091f-35e3-4289-b0XXXXXXXXXXXXXXXX: {"value":{"_type":
"RequestResponse","chunk":"
W3siSWQiOiIwIiwiU3RhdHVzIjoiTHVuY2giLCJUeXBlIjoiUmV
sYXRpdmUiLCJZZWFyIjowLCJNb250aCI6
MCwiRGF5IjowLCJIb3VyIjoxLCJNaW51dGUiOjB9LHsiSWQiO
iIxIiwiU3RhdHVzIjoiR8OldHQgZsO2ciBkYWdlbiIsIlR5cG
6MCwiRGF5IjowLCJ
Ib3VyIjoxLCJNaW51dGUiOjB9LHsiSWQ
--SNIP --
```

-"Hmm" Said Lucas out loud... This smells like BASE64
-" Whats in it?!" He did a fast BASE64 Decode...

```
{"Id":"4XX","Username":"8XXX","MobilePhone":"+4676XXXXXXX",
"OfficePhone":"+46XXXXXXXX","FirstName":"AXXXX","LastName":"
"Name":"AXXXX XXXX"},{"Id":"XXXX","Username":"2XXX"
,"MobilePhone":"+46XXXXXXXXX","OfficePhone":"+46XXXXXXXXX"
,"FirstName":"AXXXXX","LastName":" von XXXXXXX",
"Name":"AXXXXX  XXX XXXXXXX"},
```

UserIDs, Phone Numbers, Names, SESSTION TOKENS!
And from what SERVICE. Attacker can set a token... done..
There is enough info to cause severe damage
This is info transmitted LIVE!



OMFG

what kind of sorcery is this?!

```
{"Id":"4XX","Username":"8XXX","MobilePhone":"+4676XXXXXXX",
"OfficePhone":"+46XXXXXXXX","FirstName":"AXXXX","LastName":"XX
"Name":"AXXXX XXXX"},{"Id":"XXXX","Username":"2XXX"
,"MobilePhone":"+46XXXXXXXXX","OfficePhone":"+46XXXXXXXXX"
,"FirstName":"AXXXXX","LastName":" von XXXXXXX",
"Name":"AXXXXX  XXX XXXXXXX"},
```

UserIDs, Phone Numbers, Names, SESSTION TOKENS!
And from what SERVICE. Attacker can set a token... done..
There is enought info to cause severe damage
This is info transmitted LIVE!

Instead of reading the manual, and spending time on dev,
What if I just reversed the protocol when subscribing to
?

So dumping the transaction to a pcap, now what?
The Ruby script I made would be super slow scanning
the entire internet.

What is the FASTEST scanner I know?
And can I send data with that scanner?

So, without further ado...
Give a massive applause for Robert Graham's
Make a drumroll effect with your mouth

MASSCAN!

Turns out that masscan can actually send data!
How ever, I have only seen Robert getting it to work.
The Kraken only obeys its master - Or does it?

MASSCAN

Buy Mr.Graham
As many beers as
you can! Tell him
Acidgen says hi!

- Masscan is able to send data using --hello-string

- Only proof it works is from Mr.Graham
  Seen alot of non-working examples and #fails

- Ok, so lets use Roberts Examples on Iptables to get banners
  Together with some standard encapsulation in the terminal

- We also need to Base64 the binary string we reversed before

```
                                  MASSCAN
s"'^^^^^^^^^^^^^^^^^^^^^^^^^^^'"                "'^^^^^^^^^^^^^^^^^^^^^^^^^^^'"s
$[root@MeLove-U-Longtime~/]iptables -A INPUT -p tcp --dport 60000 -j DROP $
$[root@MeLove-U-Longtime~/]masscan -p1883 --hello-string'[1883]'STRING    $
$                       * Insert Hallelulia chant here *                   $
$                     Masscan default timeout 10 seconds...                $
$                   Which IMO is more than enough to get data              $
$                       DO YOU THINK I GOT ANY DATA ?!?!                   $
"s.......................................................................,s"
```

(Above question is the dumbest one yet)
(But lets not spoil anything, one step at a time)

```
*String used: ECIABk1RSXNkcAMCAA8AFHJ1Ynlncm1ybXE5eWlyMm5scHpvggYAAQABIwA==
*Other flags: --banners --source-port 60000 -oB ibm.bin --rate 100000
              --exclude 255.255.255.255
*Range:       0.0.0.0/0
```

INTERNET SCAN

MASSCAN

Current Setup: 2,8 Million results into ELK
(Elastisearch Logstash, Kibana = PAIN)
Filtering Junk: Not all 1883 are MQTT + Only Identifiable
Device Types: ActiveMQ: 4,520
Others: 14,487
Unknown: Around 40,000+

Statistics during time of writing

Total: 59,000 (Estimated Brokers)

EXAMPLE DATA

```
Tue Dec 03 11:40:12 XXX XXXXX\x9b\x01\x00\x08D:XXXXXX[XXXXXXXX][XXX]
PhXXXXXXX, PhXXXX, XaiXXXXXXXX; We have a case of infectious Lassa
fever. 1411 people are infected!; Tue Dec 03 XXXXXXXX XXX XXXXXr
\x00\x06D:XXXX[XXXXFLOO][XX] LaXXaXX, X XXX, LoXXXXXXXXXXX;
There is a expected 6.2m flood.; Tue Dec 03 XX:XX:XX XXX XXX
XX\x9a\x01\x00\xXXX:HiXXXXX[NEXXXXXX][181] HiXXXXX, HiXXXXX,
ViXXXXXXX; We have a case of maybe infectious Malaria.
599 people are infected! <-Example data from EBS (Unknown if REAL)
```

Now I have the data sent to the Broker!

This is serious enought for anyone to "listen" to
THE BIG QUESTION REMAINS - CAN I INTERACT WITH IT?
COULD I SEND "4213 PEOPLE INFECTED WITH THE ZOMBIE VIRUS" ?
BEFORE WE FIND OUT - WHAT MORE SCARY STUFF IS THERE?
HIGH-RES GRFX TIME!

INTERNET SCAN

MASSCAN

Pipeline Pressure(Control server)

```
XXXX/XXXXX/XXX: cc=CGUA&site=XXXXX&utype=TM804&loc=XXXX
22&stavgs=true&bursts=/mnt/cf/bursts/&useFTP=true&
FTPsvr=XXXXXXXXXXXXXX&FTPusr=cXXX&FTPpw=fmXXXXXXXXXXXX
XX&FTPavgs=true&useMQTT=true&MQTTpfx=XXXXXXXXX&MQTTsvr=
XXXXXXXXXXXXXXXXX&MQTTprt=1883&useFlwM=false&flowSlp=
1.XXXXXXXX&flowIcp=12.XXXXXX&presSen=IMPRESS&presSlp
=3.46455E-7&presIcp=2.505623&XXXXXXX=XXX
```

I do not want to know, whats going on here
They seem to be tracking someone

```
XXXXXXXXXXXXXXXXXXXXXX: {"tipo":"log","data":
"CANTIDAD DE SATELITE=12","id":"XXXX"}
XXXXXXXXXXXXXXXXXX: {"eventList":"{\"shock_alert\":false,
\"panic_button\":false,\"electrical_connect\":true,\"power_cut\
":false,\"battery_charge\":true,\"low_batery\":false,\"acc_on\"
:false,\"gps_tracking\":true}","ltt":"XXXXXXXXXXXXXXXXX","id":XX,
"dt":"2016-07-12 14:18:40","speed":"29","XXXXXXX":"X","command":
"XXXXXXXXXX","XXXXXXXXX":"XXXXX Ramon XXXXXXXXXXXXXXXXXXXXXXXXXXXX
 XXXXXXXXXXXXXXXXXXXXXXXXXX","recorrido":"XXXXXXXXXXXXXXXXX",
 "orientacion":"XXXXX","lng":"-XXXXXXXXXXXXXXXXX","route_meter":
 "X.XXXXXXXXXXXXXXXX","events":"N/A"}
```

Now I have the data sent to the Broker!

INTERNET SCAN

MASSCAN

Pipeline Pressure(Control server)

```
XXXX/XXXXX/XXX: cc=CGUA&site=XXXXX&utype=TM804&loc=XXXX
22&stavgs=true&bursts=/mnt/cf/bursts/&useFTP=true&
FTPsvr=XXXXXXXXXXXXXX&FTPusr=cXXX&FTPpw=fmXXXXXXXXXXXX
XX&FTPavgs=true&useMQTT=true&MQTTpfx=XXXXXXXXX&MQTTsvr=
XXXXXXXXXXXXXXXXX&MQTTprt=1883&useFlwM=false&flowSlp=
1.XXXXXXXX&flowIcp=12.XXXXXX&presSen=IMPRESS&presSlp
=3.46455E-7&presIcp=2.505623&XXXXXXX=XXX
```

I do not want to know, whats going on here
They seem to be tracking someone

```
XXXXXXXXXXXXXXXXXXXXXX: {"tipo":"log","data":
"CANTIDAD DE SATELITE=12","id":"XXXX"}
XXXXXXXXXXXXXXXXXX: {"eventList":"{\"shock_alert\":false,
\"panic_button\":false,\"electrical_connect\":true,\"power_cut\
":false,\"battery_charge\":true,\"low_batery\":false,\"acc_on\"
:false,\"gps_tracking\":true}","ltt":"XXXXXXXXXXXXXXXXX","id":XX,
"dt":"2016-07-12 14:18:40","speed":"29","XXXXXXX":"X","command":
"XXXXXXXXXX","XXXXXXXXX":"XXXXX Ramon XXXXXXXXXXXXXXXXXXXXXXXXXXXX
 XXXXXXXXXXXXXXXXXXXXXXXXXX","recorrido":"XXXXXXXXXXXXXXXXX",
 "orientacion":"XXXXX","lng":"-XXXXXXXXXXXXXXXXX","route_meter":
 "X.XXXXXXXXXXXXXXXX","events":"N/A"}
```

Now I have the data sent to the Broker!

INTERNET SCAN

MASSCAN

Cars (I think it is, since its on a road moving Lat+Long)

```
[{"t":"XXXXXXXXXXXXXXXXX","d":[{"id":
"GPS_LatLng","v":"XXXXXXXXXXXXXXX
XXXXX"},{"id":"F_SPEED","v":"81"},
{"id":"F_LON_G","v":"0.2 "},{"id":"F_ACL_POS",
"v":"81"},{"id":"F_SW_BRAKE","v":"0"},
{"id":"F_TURNR","v":"0"},{"id":"F_TURNL","
v":"0"},{"id":"F_SENSOR","v":"1"}]}]
```

Lets put all this on MQTT
1: http://XXXXXXXXX
Username: XXXXXX
Password: XXXXXX
2: Project to work
Members Registration System
Source code: http://svn.XXX.XXXXXXXXXXX
DB: http://svn.XXXXXXXX - XXXXXXXX
Project is in VS 2012 using MS Sql Server
3: Tasks List
http://jira.XXXXXXXXXXX
Your credentials are XXXXX/XXXXXXX
Start doing it according to sort order.
4: Below are your TFS credentials
http://XXXXXXXXX:8080/XXX
XXXXX/XXXXXXXXXXXX

Now I have the data sent to the Broker!

INTERNET SCAN

MASSCAN

Ok... Let's get back to more of those later
It is going to get much much worse...

Now I have the data sent to the Broker!

Do you remember the question i asked?
Can we send data to it?

OH NO

Arnold says
Bite it augh
Yeah i like it
bit.ly/29N987X

Not ONLY can we listen in on data beeing sent.

We can SEND DATA IN!

Alright, so you are mentally asking;
-"There has to be some kind of... well trust thing, that it only accepts data coming from a valid host or something? Right?"

Not to my knowledge, that is completely up to the "client" who reacts on the data.

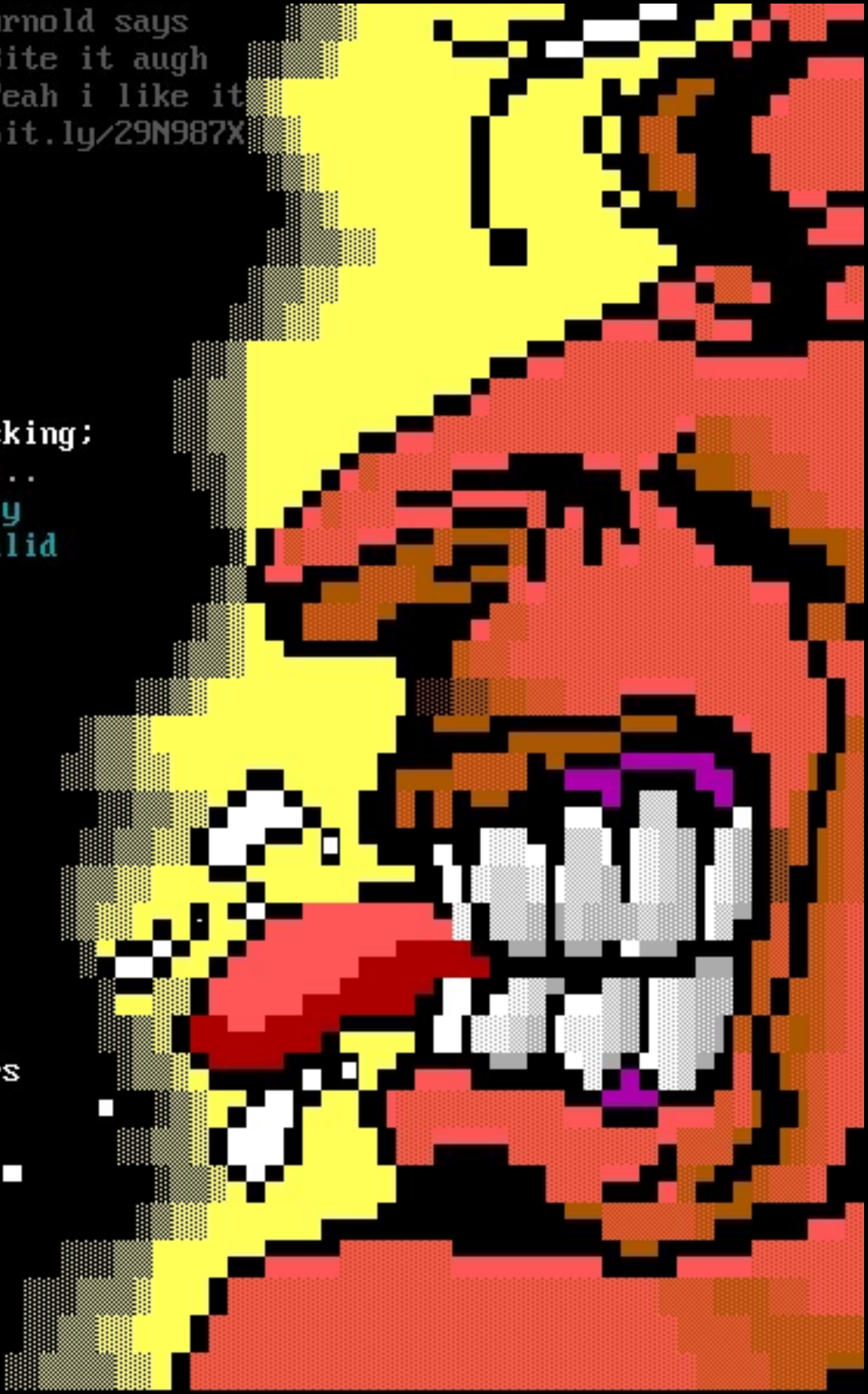
And how would the client know? It's not like there is an IP?

But But But... You can encode the data beeing sent?

Might work, sometimes.
The MQTT is installed on sensors that are Low powered, low CPU.

Might not always work.

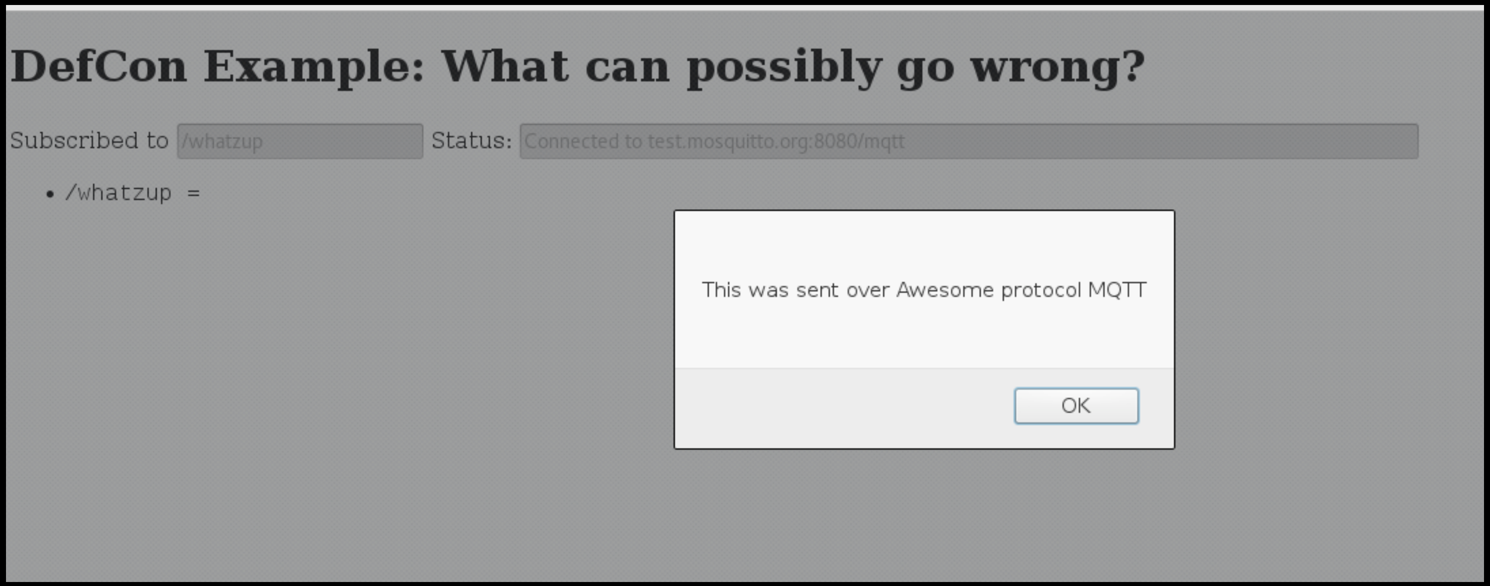
VULNS?! ARE THERE VULNS?!?!
(ARE YOU NOT ENTERTAINED?!)



XSS

XSS? Is it possible?
It would all depend on how the data is handled.
Again, let us use example code that is avalible online

HIGHRES IMG IS HERE!



DefCon Example: What can possibly go wrong?

Subscribed to /whatzup Status: Connected to test.mosquitto.org:8080/mqtt

- /whatzup =

This was sent over Awesome protocol MQTT

And I heard, as it were, the noise of thunder:
One of the four beasts saying: "Come and see." And I saw.
And behold, a vanilla XSS .

Seems like people didn't bother reading the manual? Que?
http://bit.ly/29an8Iw ◀ Source

SQLi

yomommas sql statment is so ugly
she dosen't even do sanitation' DROP * --

Looking for example code for MQTT to SQL
When I stumbled upon a MQTT Broker (Open Source)
With example code on MQTT to SQL:

No sanitation on the messages above

```
private static final String SQL_INSERT =
"INSERT INTO `Messages`
(`message`,`topic`,`quality_of_service`) VALUES (?,?,?)";
```

That means a SQLi should be possible! HA SQLi over MQTT!
Who knew right?

And I heard, as it were, the noise of thunder:
One of the four beasts saying: "Come and see." And I saw.
And behold, a vanilla SQL INJECTION.

Seems like people didn't bother reading the manual? Que?
http://bit.ly/29an8Iw ◀ Source

DadaImadeA-booboo!

whops

-Thats not good!

WHOPS - is when (using public/open brokers);

- You decided to connect your company to that MQTT broker you have
- You thought that running EBS (Emergency Broacast system) over MQTT was an awesome idea!
- The News server retrives its news from a MQTT broker
- Attaching around 15.000 ATMs to an open broken is also cool!
- Running EarthQuake alarm system getting alarms from MQTT
- Taking MQTT retrived data and pushing it directly into SQL (Lets not use any input sanitation at all)
- Using public Brokers for your Company
- Pushing Software updates via MQTT to Cars
- Installing a iPhone / Android GPS tracker to your MQTT Broker
- Exposing your bitcoin wallet throught MQTT
- Taking the MQTT data retrived and pushing it onto a Homepage
- Putting Username/Passwords/URL/IP to your development servers

OMFG

what kind of sorcery is this?!

What else can we find?
How about some ATMs ? Remember: WE CAN INTERACT!

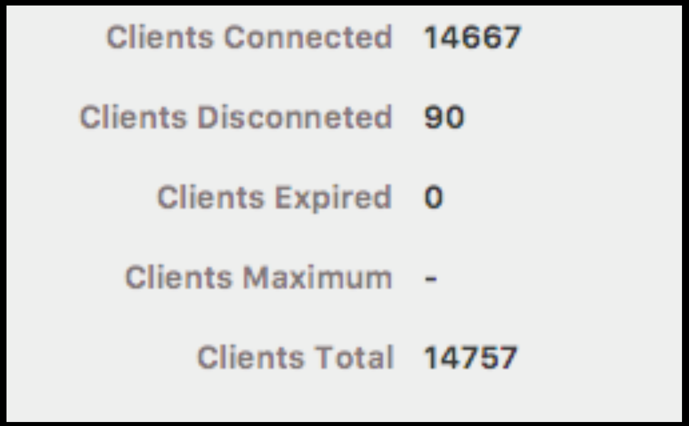
```
XXXXXXXXXXXXXXXXXXXXstatus: {"boxid":XXXX,"status":
{"OS":"Windows 5.1","bvStatus":{"states":[{"accepted"
:XXXX,"deviceId":X,"enabled":true,"errorCritical":false,
"halt":false,"id_string":"Generic CCNET VU_RU1328T
S/N XXXXXXXXXXXX","name":"Generic CCNET VU_RU1328T S/N
XXXXXXXXXXXX","rejected":582,"returned":1,"stackerFull":false,
"stackerPresent":true,"state":"busy","stateText":""}]},"
commissionFoDay":67.859999999999999,"currentDt":"XXXX-XX-
XXXXXXXXXXXX","cycle":{"comission":1092.1700000000001,
"docsFoCycle":87,"from":"XXXXXXXXXXXXXXXXXXXX","fromDoc":XXXX,
"moneys":{"bills":[{"count":1,"nominal":10},{"count":39,
"nominal":50},{"count":80,"nominal":100},{"count":3,
"nominal":500},{"count":2,"nominal":1000}],"coins":
[{"count":16,"nominal":1},{"count":25,"nominal":2},{"count":61
,"nominal":5},{"count":68,"nominal":10}]},"number":14,
"summ":13418.83},"dayTrafficIn":1296206,"dayTrafficOut"
:1703336,"docNumber":1697,"docsForDay":6,"freeDisk":"E:\\
43 GB/55 GB","fullStartDt":"XXXXXXXXXXXXXXXXXXXZ",
"insertedSummForDay":754,"lastActivity":
"XXXXXXXXXXXXXXXXXXXX","lastPayoutDt":"XXXXXXXXXXXXXXXXXXXX"
,"lastPayoutSumm":10514,"lastTouchClick":"13 Jul 2016 XXXXXXXX
 XXXXX","modem":{"balance":100,"balanceText":"Balans:100XX
 Limit:0,01XX","locations":[{"cid":"","lac":
"","mcc":"250","mnc":"01"},{"cid":"0","lac":
"0","mcc":0,"mnc":0},{"cid":"XXXXX","lac":"XXXXX","mcc":XXX,
"mnc":1},{"cid":"0","lac":"XXXXX","mcc":250,"mnc":1},{"cid":"0
"lac":"XXXXX","mcc":250,"mnc":1},{"cid":"0","lac":"XXXXX","mcc
250,"mnc":1}],"modemName":"SIEMENS MC35i REVISION 01.10_7d6c",
--SNIP--
```

OMFG

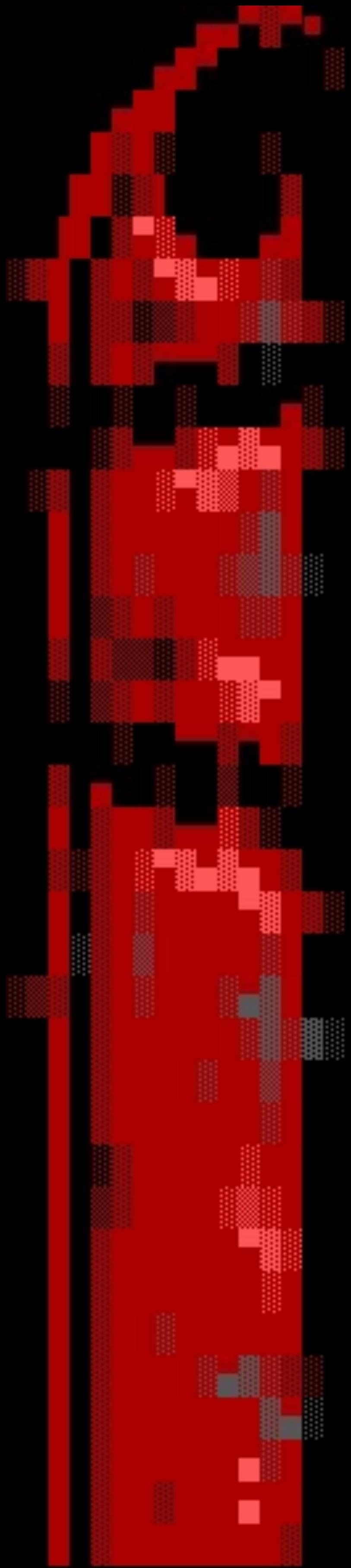
what kind of sorcery is this?!

What else can we find? *Phew, Getting Hot In here...*
So, how many ATMs you ask?
Around the 14,000 Mark. How do i know?
MQTT if using a popular Broker allows me to query it
Subscribing to # with e.g MQTT.fx will crash it
it's too much data!

SCREENSHOT HERE:



Clients Connected	14667
Clients Disconneted	90
Clients Expired	0
Clients Maximum	-
Clients Total	14757



OMFG

what kind of sorcery is this?!

What else can we find?
I will just make a sum, and you can take my word for it

Prisons
Cars
Car Firmware (Entertainment system)
Alarms (HVAC etc)
Personal Tracking information (owntracks)
Fitness bands
Medical Equipment
Bitcoin info
Session tokens
Usernames / Passwords / Social Security numbers
URLs to obscure pages
Power Meters
Radiation Meters
Air Condition / Humidity control
Flight Information (Lat,long,speed,Direction,name,etc)
GeoGraphical Data (EarthQuakes, etc)
MMORPG (Stats, armour, Abilities etc)
Messaging apps (All users talking on a Messaging app,phone)
Raw data (Base64 encoded, images, audiofiles etc)
SQL Statments (wtf?)
GPS tracking (cars, boats, planes, people)
... There is soo much in there... its scary ...

Now Devs are ranting : But you are not supposed to connect
this, only when testing.

Yeah of course, but there is a difference between should
and whats really going on...

BOTNET

Your mind works best under struggle (or so they say, by they I mean me),
so when I was at the toilet...this hit me;

- MQTT is designed to send data to multiple hosts
  This is done with as minimal bandwith as possible

- There are thousands of thousand of MQTT Brokers
  An attacker can choose almost anyone of these Brokers
  Or even Switch Broker if one is down

- If I where to design an example, it should work
  On both Linux / Windows etc etc

- No more need for "pesky" IRC channels any more
  I can use the MQTT Topics

So, this is what I did....
DEMO DEMO DEMO DEMO DEMO DEMO DEMO
THE WORLDS FIRST (?perhaps) Backdoor/Botnet over MQTT

Seems like people didn't bother reading the manual? Que?
http://bit.ly/29an8Iw ◄ Source

THANK YOU!

THANK YOU

There are some honorable mentions:

MY.KIDS	Kid1,Kid2,Kid3 (You rock)
MY.WIFE	Thank you for putting up with me
roy/SAC	roy/SAC (www.roysac.com) ANSI
NIKI7A	Thanks for the time extension
NEAL.HINADOCHA	Thanks for talking me into it
DARK.TANGENT	DefCon Founder
MARC.THIELE	ANSI Stuff
ACID	They made Awesome ANSI
KYPRIANOS	Thanks for listening to me
MICHELE.ORRU	The Italian Stallion
ZYPZYP	King ZypZyp (a.k.a the baws)
PIOTR.DYZ..Dy..ahh.fuck.it	Thanks for helping out
FORTCONSULT	My Collegues and friends
GI0TIS	Souvlaki brother
C0RELANC0D3R	Adopt me
PEOPLE.I.FORGOT	SORRY!
ROBERT.GRAHAM	(M)ASSCAN!, It R0x0rs!
HDM	Make a MQTT Meterpreter :D

AND A VERY SPECIAL THANK YOU
TO YOU PEOPLE
FEEL FREE TO HIT ME UP
@acidgen

Lets make the Internet Secure again