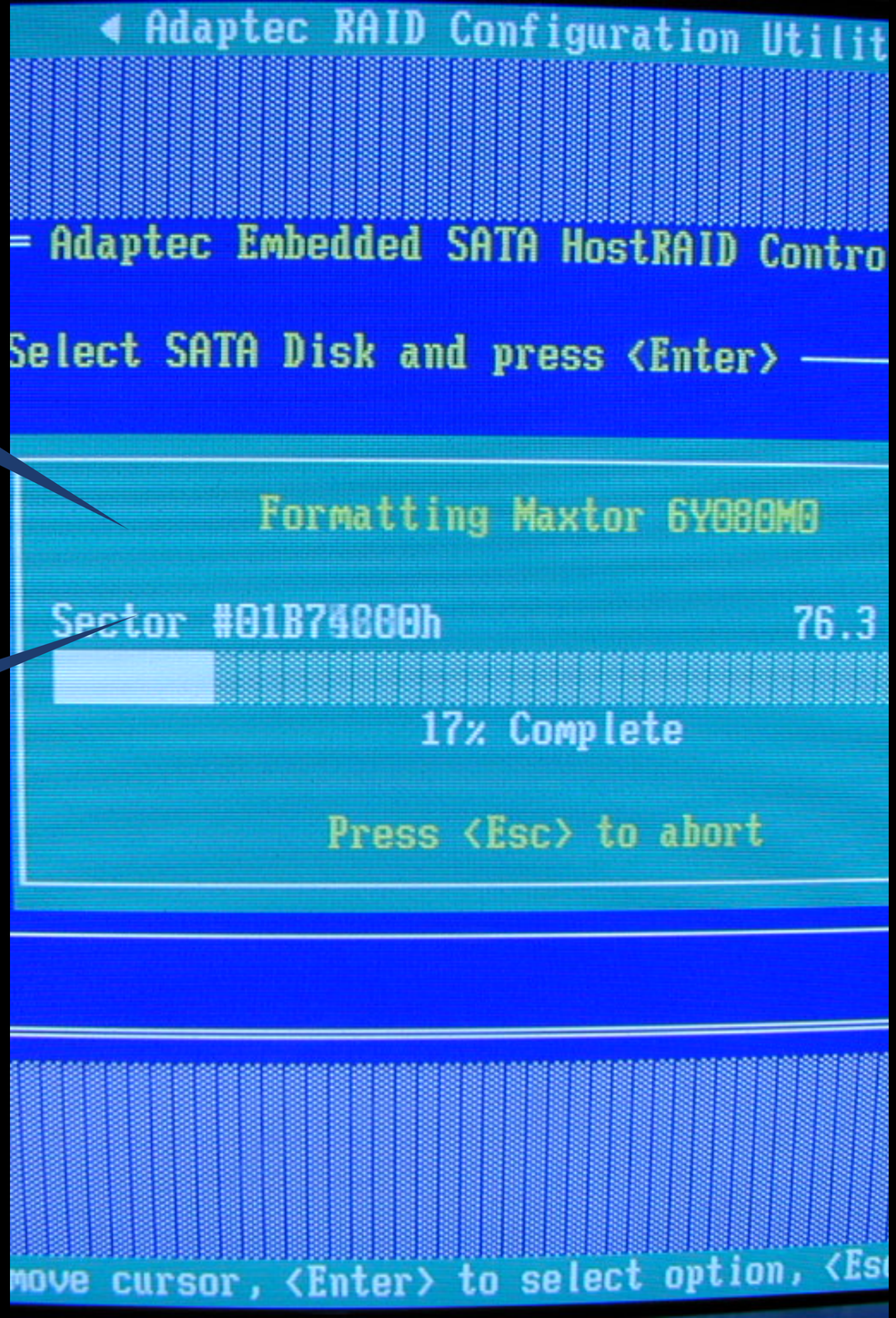
STIBBE SEMINAR

INSURANCE AGAINST CYBERCRIME

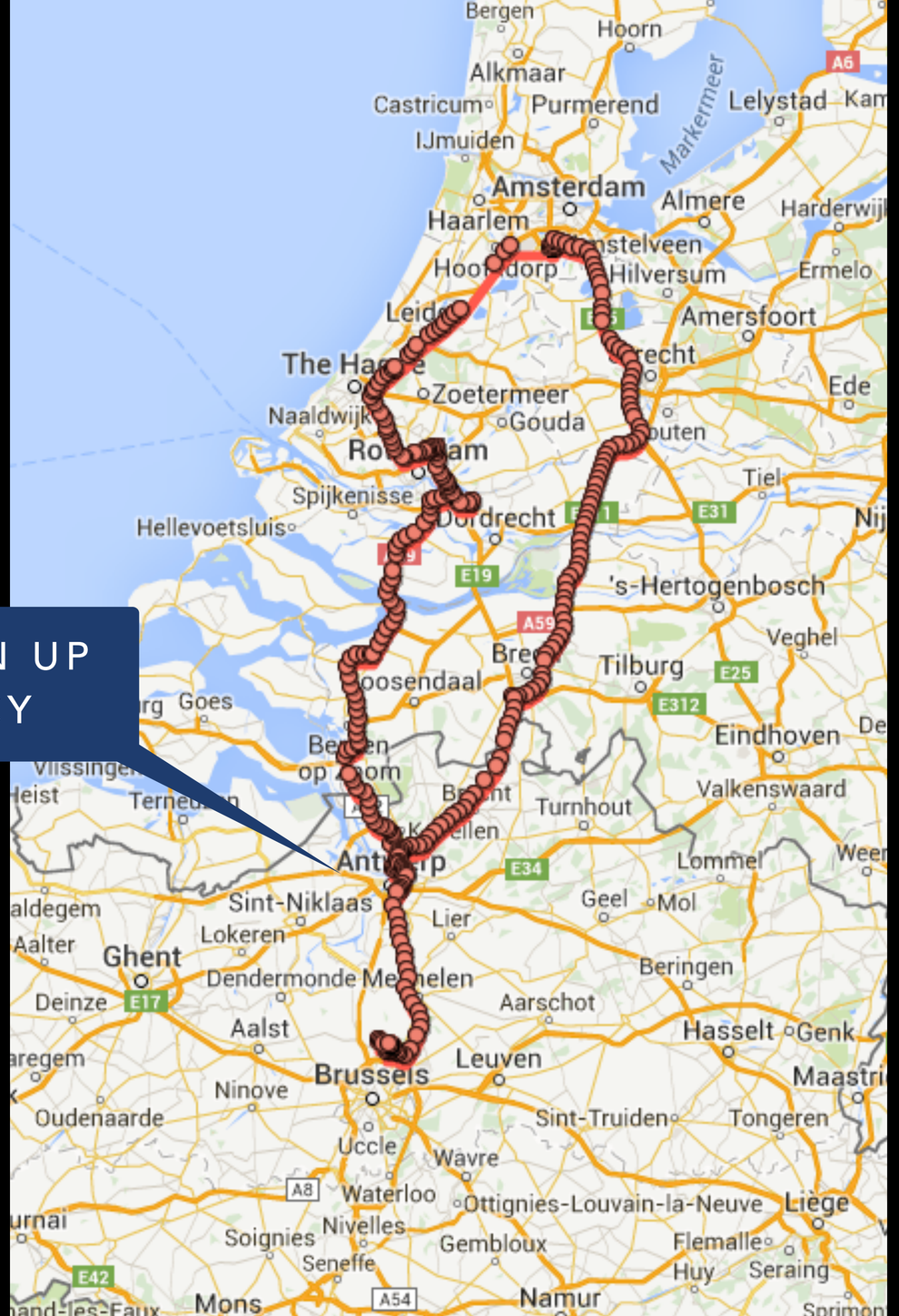
HI, MY NAME IS
YERI TIETE

I GREW UP WITH THE INTERNET WHEN SECURITY WAS IRRELEVANT

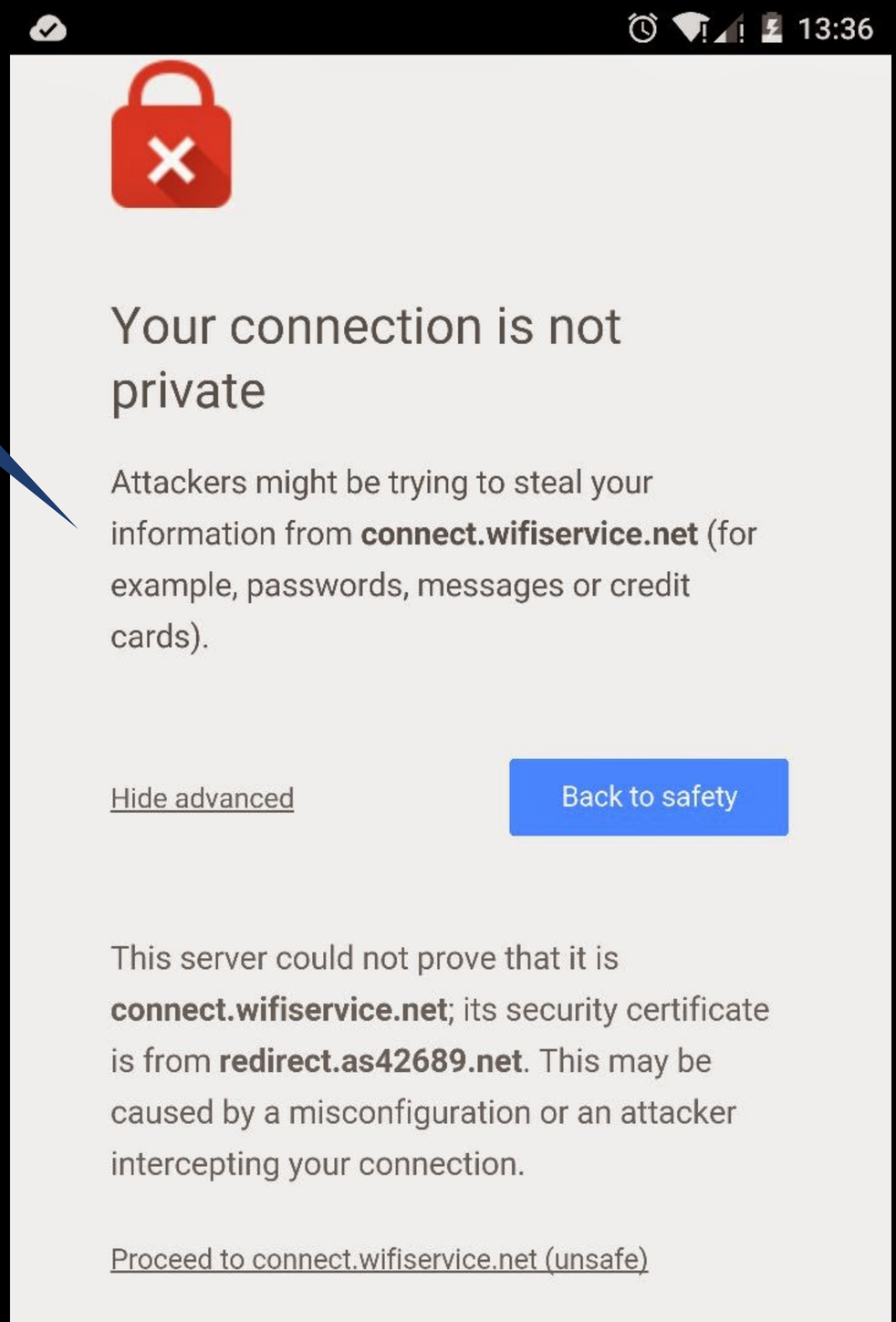
I RECEIVED DECOMMISSIONED HOSPITAL DESKTOPS — USUALLY STILL FULL OF PATIENT DETAILS



I HAVE GIVEN UP ON PRIVACY



WE UNDERESTIMATE THE NUMBER OF ATTACKS AND THE INFORMATION WE LEAK



AND WE'VE LOST COUNT OF THE INTERNET CONNECTED DEVICES

THE TOOLS

FREE & OPEN SOURCE

World's most used penetration testing software

Put your network's defenses to the test

A collaboration of the open source community and Rapid7. Our penetration testing software, Metasploit, helps verify vulnerabilities and manage security assessments.

FREE METASPLOIT DOWNLOAD LEARN MORE

Get free Nexpose Vulnerability Scanner

Metasploit integrates with Nexpose to verify vulnerabilities

FREE NEXPOSE DOWNLOAD

KALI LINUX™

"the quieter you become, the more you are able to hear"

Blog Downloads Training Documentation Community About Us

Our Most Advanced Penetration Testing Distribution, Ever.

Kali Linux - A Flexible Penetration Testing Platform

From the creators of BackTrack comes **Kali Linux**, the most advanced and versatile **penetration testing distribution** ever created. We have a whole set of amazing features lined up in our security distribution geared at streamlining the penetration testing experience.

Read More

https://www.shodan.io/search?query=IN-TANK+

Shodan Scanhub Developers View All...

SHODAN IN-TANK Explore Membership Contact Us Blog Enterprise Access

Exploits Maps Download Results Create Report

DEFAULT USER & PASS:
HTTP://WWW.PHENOELIT.ORG/DPL/DPL.HTML

TOP COUNTRIES

United States	3,400
Korea, Republic of	55
Germany	29
Puerto Rico	26
New Zealand	26

TOP SERVICES

Automated Tank Gauge	3,539
NetBIOS	89
SMB	38
FTP	29
SSH	9

TOP ORGANIZATIONS

Comcast Business Communications	299
CenturyLink	257
Comcast Cable	233
AT&T U-verse	228
Optimum Online	155

TOP OPERATING SYSTEMS

FreeBSD 8.x	1

TOP PRODUCTS

OpenSSH	16
MongoDB	10
ProFTPD	9
Apache httpd	8
Ventrilo	5

Showing results 1 - 10 of 3,852

66.201.152.144

Visionary Communications

Added on 2015-05-04 12:38:40 GMT

United States, Spokane

Details

```
I20100
05/04/15  6:23 AM

BIG D #11
402 MAIN ST
DEADWOOD SD 57732
605=578=1110

IN-TANK INVENTORY

TANK PRODUCT               VOLUME TC-VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  UNLEADED                1851         0     9831    20.70     0.00    50.64
  2  UNLEADED 2          ...
```

208.157.149.222

Cable & Wireless (Cayman Islands)

Added on 2015-05-04 12:34:16 GMT

Cayman Islands, George Town

Details

```
I20100
04/05/15  7:22

WALKERS ROAD RUBIS


IN-TANK INVENTORY

TANK PRODUCT               VOLUME TC-VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  DIESEL                   501         0     4495    16.36     0.00    87.38
  2  PREMIUM                 7850         0      477    81....
```

69.179.85.141

69-179-85-141.stat.centurytel.net

CenturyLink

Added on 2015-05-04 12:21:41 GMT

United States

Details

```
I20100
MAY  4, 2015  7:49 AM

BLACK RIVER CROSSING
```

DEMO TIME

WEBSITES

HTTPS://WWW.SHODAN.IO/SEARCH?QUERY=TITLE%3A%22HACKED+BY%22

Hacked by El Moujahidin

#Free Hamza Bendelladj #Free Palestine

Tell Your Gov , To Know About Palestine

We Will Countinue Hacking The Sites , To Send The Message Of Our Palestine And All Arabs

We Dont Accept Killing Muslims Evry Where, Stop Killing US

#We Are El Moujahidin Team We Will Not End This War

#AttaCker fr0m #Algeria

son ~ Matrix Dz ~ Ouss_Dz ~ Admirale_Mouh ~ Lahcen NB ~ Mr Dz ~ Daya iLLi ~ AmRocky-Dz9

Fuck USA & israel .

SURVEILLANCE

HTTPS://WWW.SHODAN.IO/SEARCH?QUERY=WEBCAMXP

CONSTRUCTION SITE? HTTP://217.193.142.170:8080/
PRIVATE HOUSE? HTTP://80.229.253.103:8080/ & HTTP://81.57.29.211:8080/
EQUIPMENT? HTTP://144.92.230.77/VIEW/VIEWER_INDEX.SHTML?ID=509037 & HTTP://80.87.129.59/VIEW/INDEX.SHTML
OFFICE? HTTP://208.13.138.33/VIEW/INDEX.SHTML
PARKING? HTTP://208.67.229.99/VIEW/VIEWER_INDEX.SHTML?ID=13016
A CITY? HTTP://46.228.50.142/VIEW/INDEX.SHTML

PRINTERS

HTTPS://WWW.SHODAN.IO/SEARCH?QUERY=PRODUCT%3A%22HP+LASERJET+P2055+SERIES%22

HTTP://136.183.4.187/
HTTP://129.128.93.54/
HTTP://75.147.242.162/SSI/INDEX.HTM

NETWORK STORAGE

HTTPS://WWW.SHODAN.IO/SEARCH?QUERY=IOMEGA

HTTPS://107.7.206.197/INDEX.HTML
HTTPS://71.100.173.70/INDEX.HTML
HTTPS://24.132.238.91/FOLDERCONTENT.HTML?FOLDER=PICTURES (PICTURES > 100NIKON > 0034.JPG)

NETWORK DEVICES

HTTPS://WWW.SHODAN.IO/SEARCH?QUERY=TP-LINK

HTTP://46.238.40.218:8080/ (ADMIN:ADMIN)
HTTP://95.111.77.188:8080/
HTTP://78.90.42.102:8080/

WELL, SO FAR IT WAS MOSTLY END USER EQUIPMENT
HOW ABOUT FUEL STATIONS ?

HTTPS://WWW.SHODAN.IO/SEARCH?QUERY=FUEL

TELNET <IP> 10001
(CTRL+A) I20100

216.255.6.221
72.66.114.139

```
I20100
MAY  4, 2015  9:47 AM

104021 CITGO EXPRESS
520 S.PAINT ST.
CHILLICOTHE,OH
80548703205001

IN-TANK INVENTORY

TANK PRODUCT               VOLUME TC VOLUME   ULLAGE   HEIGHT    WATER     TEMP
  1  UNLEADED 1                4905      4921     5095    47.28     0.91    55.01
  2  UNLEADED 2                4901      4919     5099    47.25     1.22    54.49
  3  SUPER                     1478      1483     8522    19.71     0.00    55.03
  4  RACING FUEL                562       561     1938    17.67     0.00    61.99
  5  DIESEL                     536       536      467    33.73     0.00    57.27
  6  K-1                        622       623      381    38.07     0.00    56.18
```

WIND FARMS

HTTPS://WWW.SHODAN.IO/SEARCH?QUERY=JETTY+2000

HTTP://63.68.133.61/13_04_01/INDEX_EN.JSP
HTTP://213.58.174.220/11_06_11/INDEX_EN.JSP
HTTP://176.227.140.112/1_08_02/INDEX_EN.JSP

SQL INJECTIONS

HTTPS://WWW.GOOGLE.BE/SEARCH?IE=UTF-8&Q=SITE:FGOV.BE+SQL&GWS_RD=CR&EI=W71DVDRKIYFXAIPUGJAD

HTTP://WWW.EJUSTICE.JUST.FGOV.BE/CGI_LOI/LOI_A1.PL?DETAIL&EQUALS;1804032130%2FF&CALLER&EQUALS;LIST&ROW_ID&EQUALS;1&NUMERO&EQUALS;11&RECH&EQUALS;14&CN&EQUALS;1804032130&TABLE_NAME&EQUALS;LOI&NM&EQUALS;1804032150&LA&EQUALS;F&DT&EQUALS;CODE+CIVIL&LANGUAGE&EQUALS;FR&FR&EQUALS;F&CHOIX1&EQUALS;ET&CHOIX2&EQUALS;ET&FROMTAB&EQUALS;LOI_ALL&TRIER&EQUALS;PROMULGATION&CHERCHER&EQUALS;T&SQL&EQUALS;DT+CONTAINS++%27CODE%27%26+%27CIVIL%27AND+ACTIF+%3D+%27Y%27&TRI&EQUALS;DD+AS+RANK+&IMGCN.X&EQUALS;34&IMGCN.Y&EQUALS;10

WIFI

Destination	Protocol	Port	% Usage	Usage ▾	Sent	Received	Flows	Active time
www.googleapis.com	UDP	443	20.8%	127.8 MB	121.4 MB	6.4 MB	107	11 hours
81.165.7.59	UDP	41219	13.0%	79.7 MB	37.6 MB	42.1 MB	1	2 hours
mail.rootspirit.com	TCP	993	4.9%	30.3 MB	9.3 MB	21.0 MB	2563	13 hours
Google	-	-	4.7%	29.1 MB	11.1 MB	18.0 MB	2259	2.3 days
android.googleapis.com	TCP	443	4.0%	24.8 MB	9.3 MB	15.5 MB	526	15 hours
185.60.216.2	UDP	3478	3.1%	18.9 MB	8.8 MB	10.1 MB	6	43 minutes
www.googleapis.com	TCP	443	3.0%	18.3 MB	10.2 MB	8.1 MB	957	26 hours
r17---sn-5hnezn7y.gvt1.com	TCP	443	3.0%	18.3 MB	461 KB	17.9 MB	2	2 minutes
Google HTTPS	-	-	2.9%	17.6 MB	5.0 MB	12.5 MB	810	23 hours
android.googleapis.com	UDP	443	2.6%	15.7 MB	14.8 MB	863 KB	7	25 minutes
imap.flatturtle.com	TCP	993	2.2%	13.5 MB	3.5 MB	10.0 MB	1151	6.5 hours
fonts.gstatic.com	TCP	443	2.2%	13.3 MB	632 KB	12.7 MB	30	21 minutes
play.googleapis.com	UDP	443	1.9%	11.6 MB	11.0 MB	619 KB	3	14 minutes
r16---sn-5hneznee.gvt1.com	TCP	443	1.8%	11.2 MB	238 KB	11.0 MB	1	60 seconds
doc-0-0-sj.sj.googleusercontent.com	TCP	443	1.8%	11.1 MB	128 KB	10.9 MB	1	60 seconds

	Status	Description	Last seen	Usage ▾	OS	IPv4 address	Policy
1		iPhone	May 05 14:13	47.4 MB	Apple iOS	10.141.67.186	normal
2		iPhone-6-Steven	May 05 14:16	37.6 MB	Apple iOS	10.196.55.108	normal
3		iPad	May 05 14:16	1.3 MB	Apple iOS	10.24.136.124	normal
4		android-a737ed2a0553fa16	May 05 14:08	1.3 MB	Android	10.210.186.205	normal
5		android-710cb95b8fbaf17	May 05 14:15	1.1 MB	Android	10.87.243.240	normal
6		android-ad9f61ad2338eb75	May 05 14:15	979 KB	Android	192.168.2.43	normal
7		android-2a392f9225a3e7d	May 05 14:15	23 KB	Android	10.98.73.229	normal

SOLUTIONS?

NO EASY FIX

- PROCESS
- SECURITY THROUGH OBSCURITY DOESN'T WORK
- UNDERSTAND YOU ARE ALWAYS VULNERABLE
- SECURITY BUDGET != IT BUDGET
- DEFINE KEY ASSETS & IP
  - MANAGEMENT (NOT IT)
  - FOCUS ON THOSE
- BOUNTY + ETHICAL HACKING (HTTPS://HACKERONE.COM/)
- CREATE AWARENESS; SOCIAL ENGINEERING STILL BIGGEST ENTRY POINT (IE: BADUSB)


THANKS!
Get in touch?
Yeri@FlatTurtle.com
+32 474/61 01 39
linkedin.com/in/yeritiete