FROM CHINA WITH LOVE

by Oleg Kupreev & Nikita Tarakanov

WHO IS OLEG KUPREEV?

- Russian Security Researcher
- Hardware researching
- Software researching
- Reverse engineering
- Exploit development

WHO IS NIKITA TARAKANOV?

- ❖ Independent Russian Security Researcher
- ❖ Aka Vulnerability Assassin
- ❖ Aka Crazy Wild Russian
- ❖ Aka Stars Alinger
- ❖ Nice dude ☺

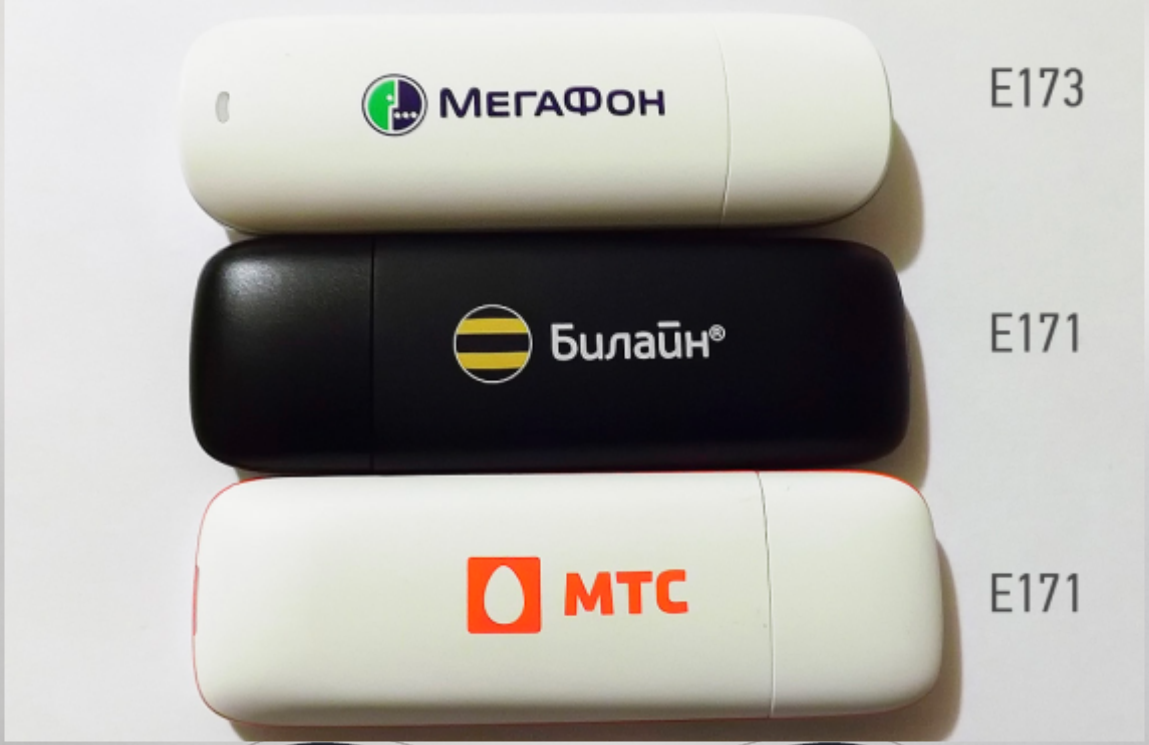
AGENDA

- **Hardware** overview
- **Software** overview
- **Infection ideas**
- **Pwning ideas**
- **Conclusion**
- **Q&A**

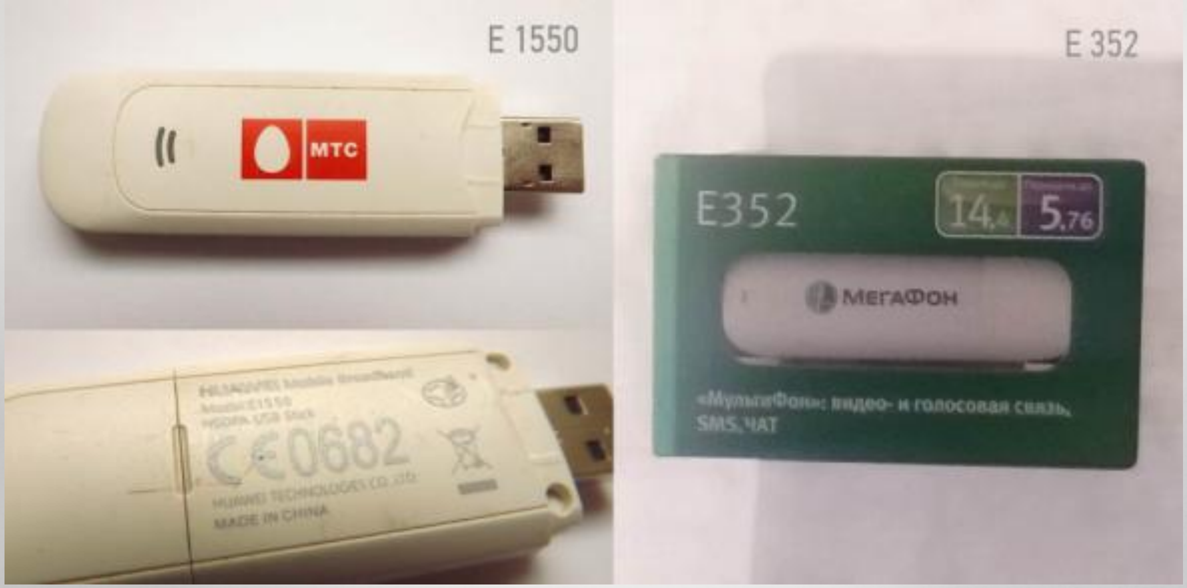
HARDWARE

- **Many** Mobile Partners (Beeline, Megafon, MTS, T-Mobile, Vodafone) users in different countries
- **One** modem vendor - HUAWEI
- **One** SOC vendor – Qualcomm

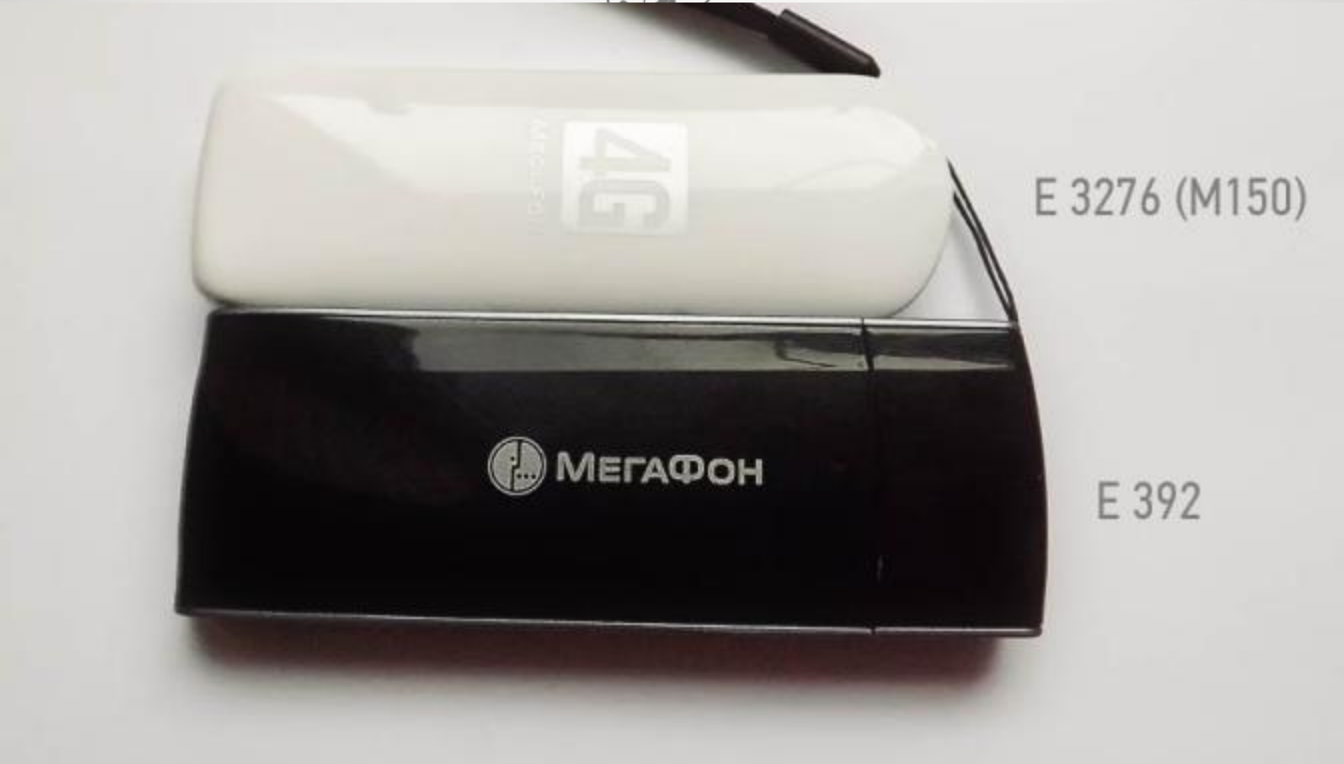
3G MODEMS



MORE 3G MODEMS



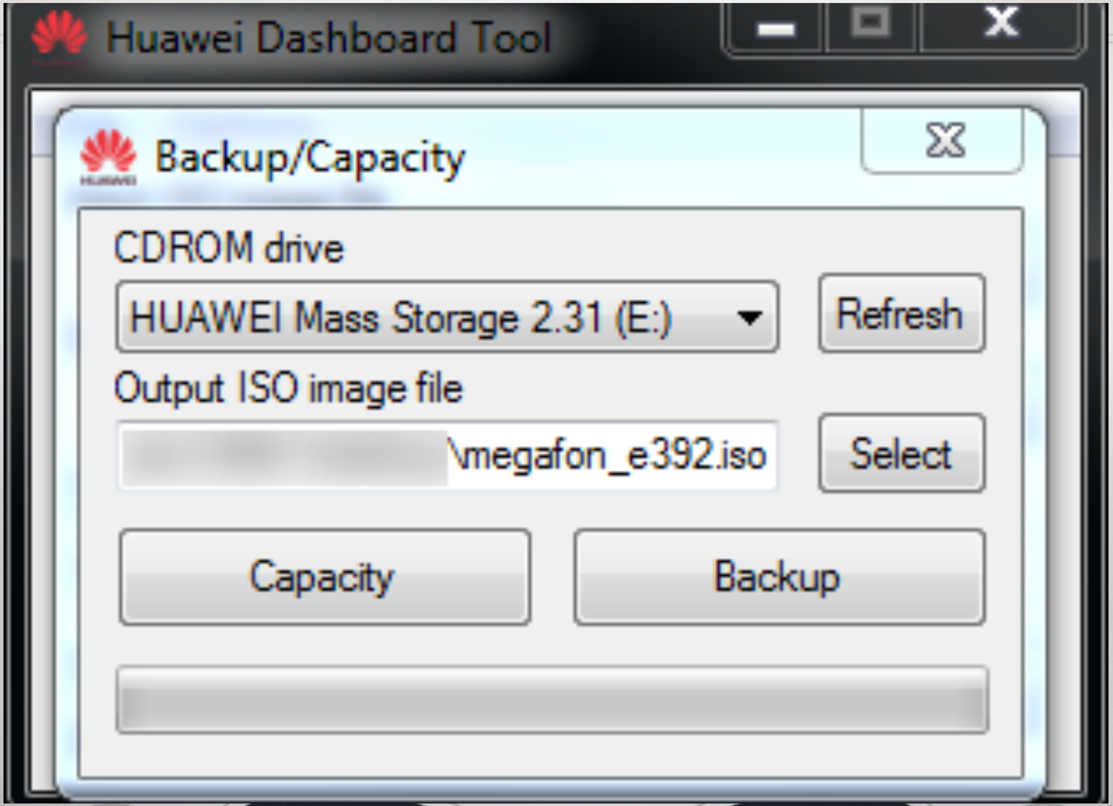
4G LTE MODEMS



VENDOR SOFTWARE

- Huawei Dashboard Tool for ISO dumping and executable dashboard generation
- Qualcomm QPST,QXDM,QMAT are used for all kind of baseband reverse engineering

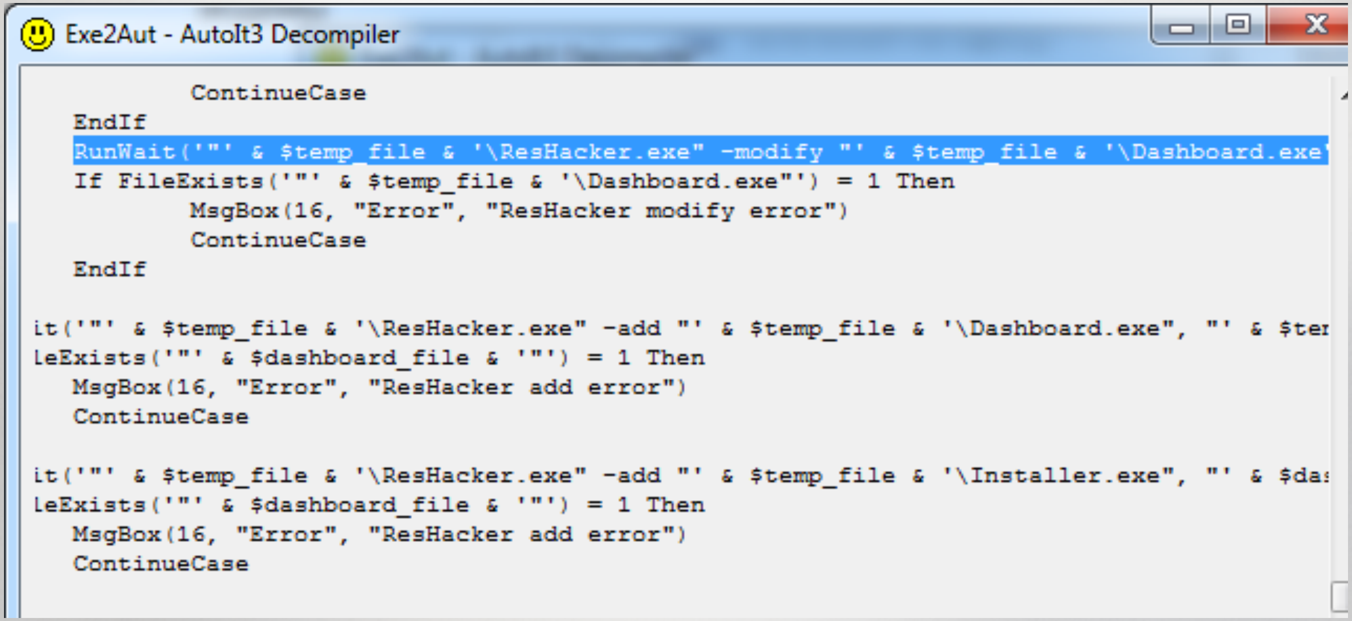
HUAWEI TOOL



CDROM drive: HUAWEI Mass Storage 2.31 (E:)

Output ISO image file: [redacted]\megafon_e392.iso

HUAWEI_TOOL.AU3



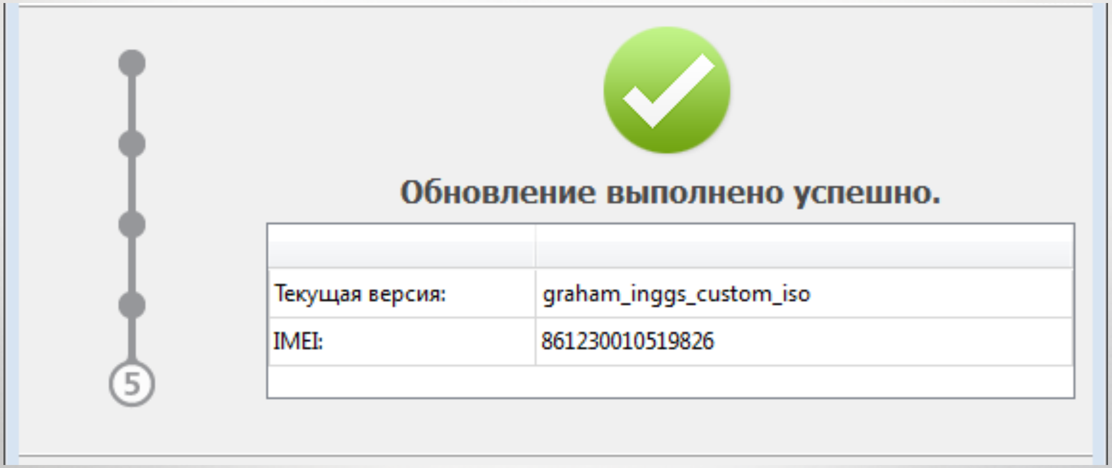
Exe2Aut - AutoIt3 Decompiler

```
            ContinueCase
    EndIf
    RunWait('"' & $temp_file & '\ResHacker.exe" -modify "' & $temp_file & '\Dashboard.exe'
    If FileExists('"' & $temp_file & '\Dashboard.exe"') = 1 Then
            MsgBox(16, "Error", "ResHacker modify error")
            ContinueCase
    EndIf

it('"' & $temp_file & '\ResHacker.exe" -add "' & $temp_file & '\Dashboard.exe", "' & $ter
leExists('"' & $dashboard_file & '"') = 1 Then
    MsgBox(16, "Error", "ResHacker add error")
    ContinueCase

it('"' & $temp_file & '\ResHacker.exe" -add "' & $temp_file & '\Installer.exe", "' & $das
leExists('"' & $dashboard_file & '"') = 1 Then
    MsgBox(16, "Error", "ResHacker add error")
    ContinueCase
```

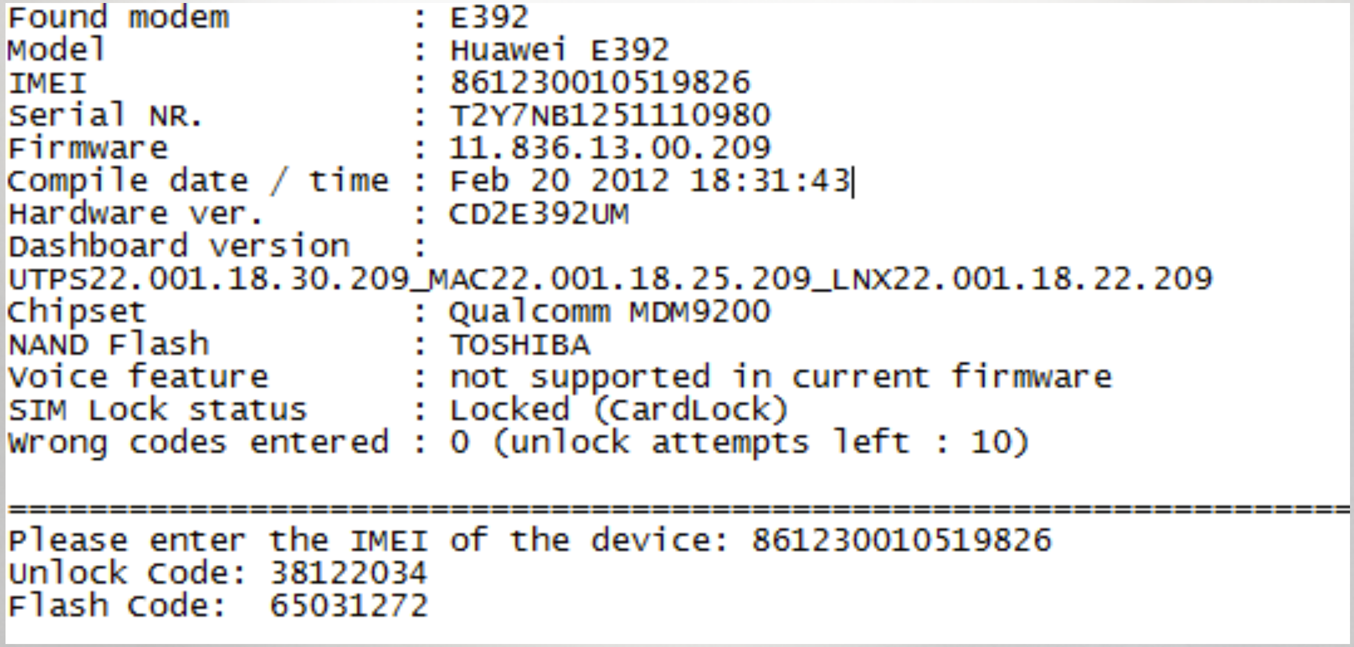
DASHBOARD UPDATABLE!



Обновление выполнено успешно.

Текущая версия:	graham_inggs_custom_iso
IMEI:	861230010519826

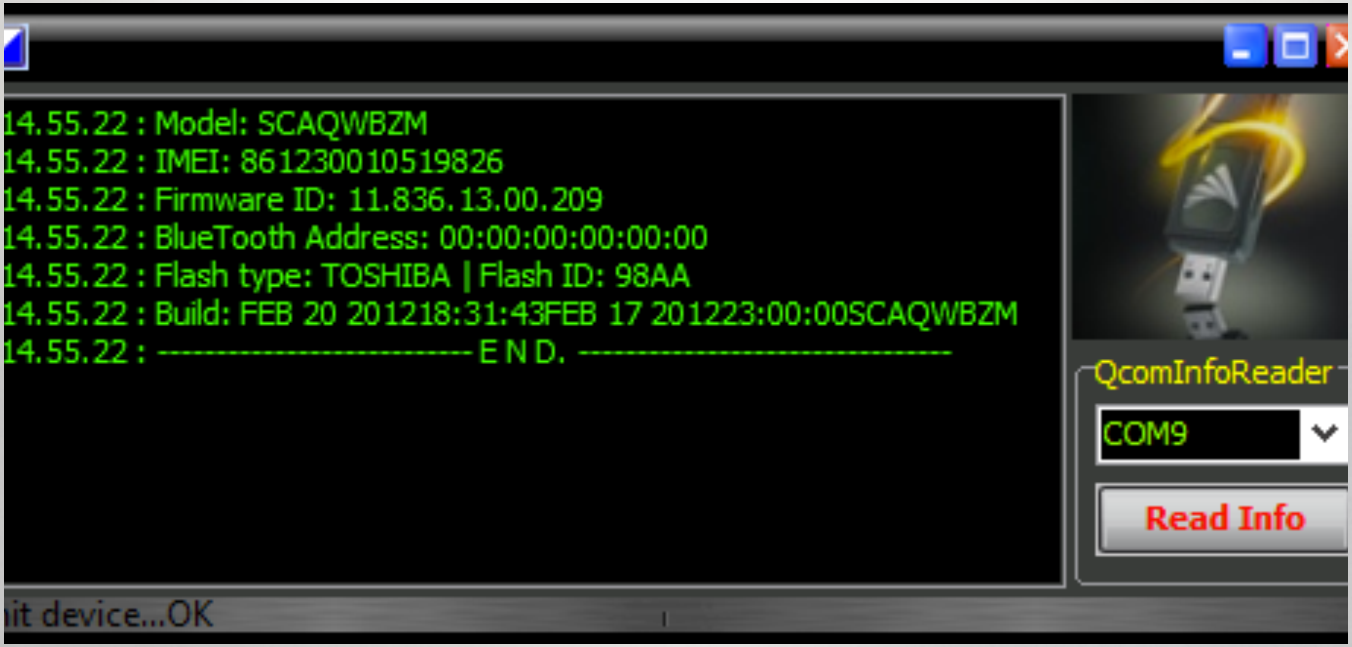
UNLOCK LOG



```
Found modem          : E392
Model                : Huawei E392
IMEI                 : 861230010519826
Serial NR.           : T2Y7NB1251110980
Firmware             : 11.836.13.00.209
Compile date / time  : Feb 20 2012 18:31:43
Hardware ver.        : CD2E392UM
Dashboard version    :
UTPS22.001.18.30.209_MAC22.001.18.25.209_LNX22.001.18.22.209
Chipset              : Qualcomm MDM9200
NAND Flash           : TOSHIBA
Voice feature        : not supported in current firmware
SIM Lock status      : Locked (CardLock)
Wrong codes entered  : 0 (unlock attempts left : 10)

===================================================================
Please enter the IMEI of the device: 861230010519826
Unlock Code: 38122034
Flash Code:  65031272
```

QUALCOMM INFO



```
14.55.22 : Model: SCAQWBZM
14.55.22 : IMEI: 861230010519826
14.55.22 : Firmware ID: 11.836.13.00.209
14.55.22 : BlueTooth Address: 00:00:00:00:00:00
14.55.22 : Flash type: TOSHIBA | Flash ID: 98AA
14.55.22 : Build: FEB 20 201218:31:43FEB 17 201223:00:00SCAQWBZM
14.55.22 : ------------------------------- E N D. --------------------------------
```

QcomInfoReader

COM9

it device...OK

HARDWARE SUMMARY

Modem	Network	Qualcomm SOC	CD-ROM capacity
E1550	2G/3G	MSM6246	64MB
E171	2G/3G	MSM6290	128MB
E173	2G/3G	MSM6290	128MB
E352	2G/3G	MSM6290	128MB
E392	2G/3G/4G LTE	MDM9600	256MB
E3276 (M150)	2G/3G/4G LTE	MDM9225	128MB

HOMEBREW SOFT

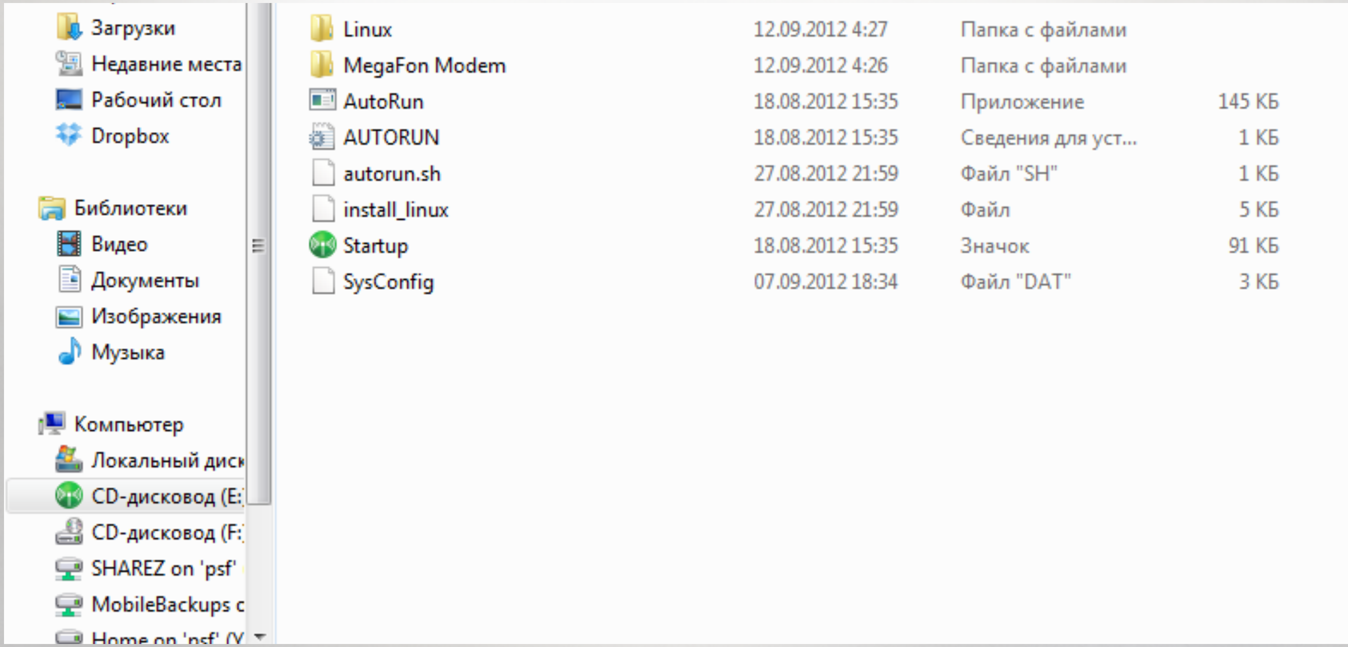
- Different Unlockers (DC-Unlocker, Huawei Modem Unlocker 5.8.1 by Bojs, Huawei Calculator, Huawei NCK Calc)
- QcomInfoReader
- Custom dashboards
- Custom baseband firmwares

MOBILE PARTNER CD

Dialing software and modem drivers are stored at hybrid CD image (ISO9660/HFS+) and contains:

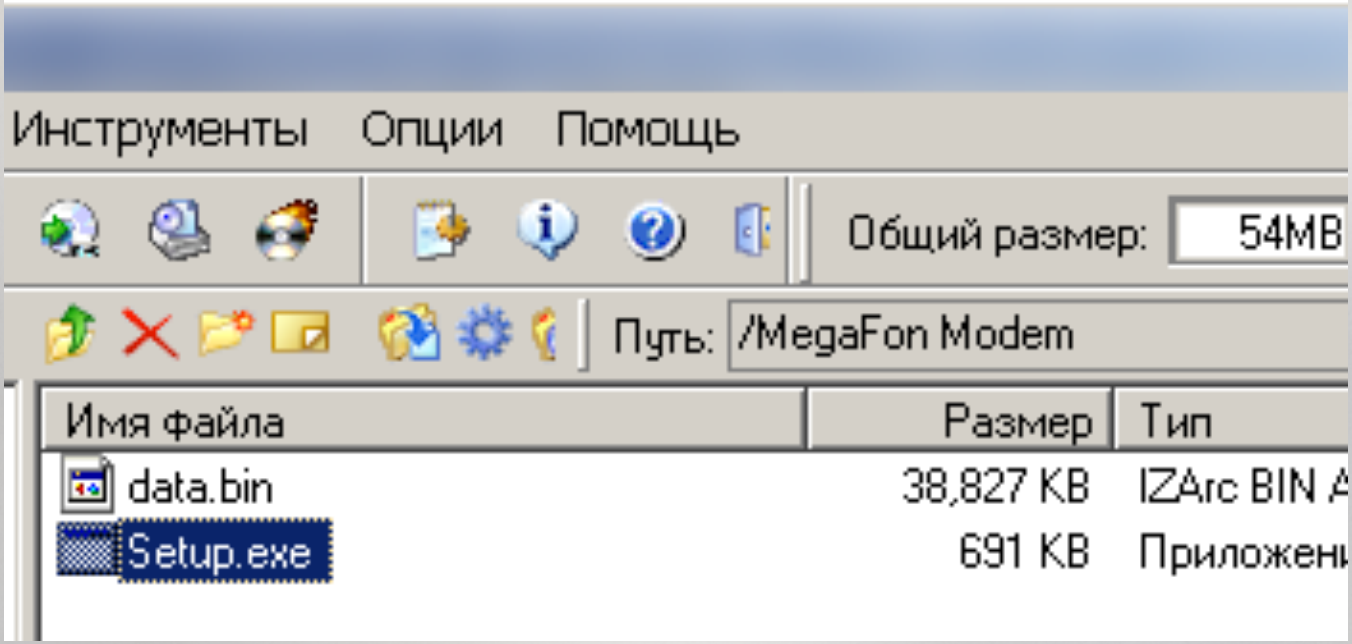
- Mobile Partner (lots of misc stuff) and **drivers** for Windows
- Mobile Partner installation **script** for Linux
- Mobile Partner **app** for OS X
- **Windows + Linux + OS X – sweet targets to rootkit**

WINDOWS PART 1



Linux	12.09.2012 4:27	Папка с файлами	
MegaFon Modem	12.09.2012 4:26	Папка с файлами	
AutoRun	18.08.2012 15:35	Приложение	145 КБ
AUTORUN	18.08.2012 15:35	Сведения для уст...	1 КБ
autorun.sh	27.08.2012 21:59	Файл "SH"	1 КБ
install_linux	27.08.2012 21:59	Файл	5 КБ
Startup	18.08.2012 15:35	Значок	91 КБ
SysConfig	07.09.2012 18:34	Файл "DAT"	3 КБ

WINDOWS PART 2

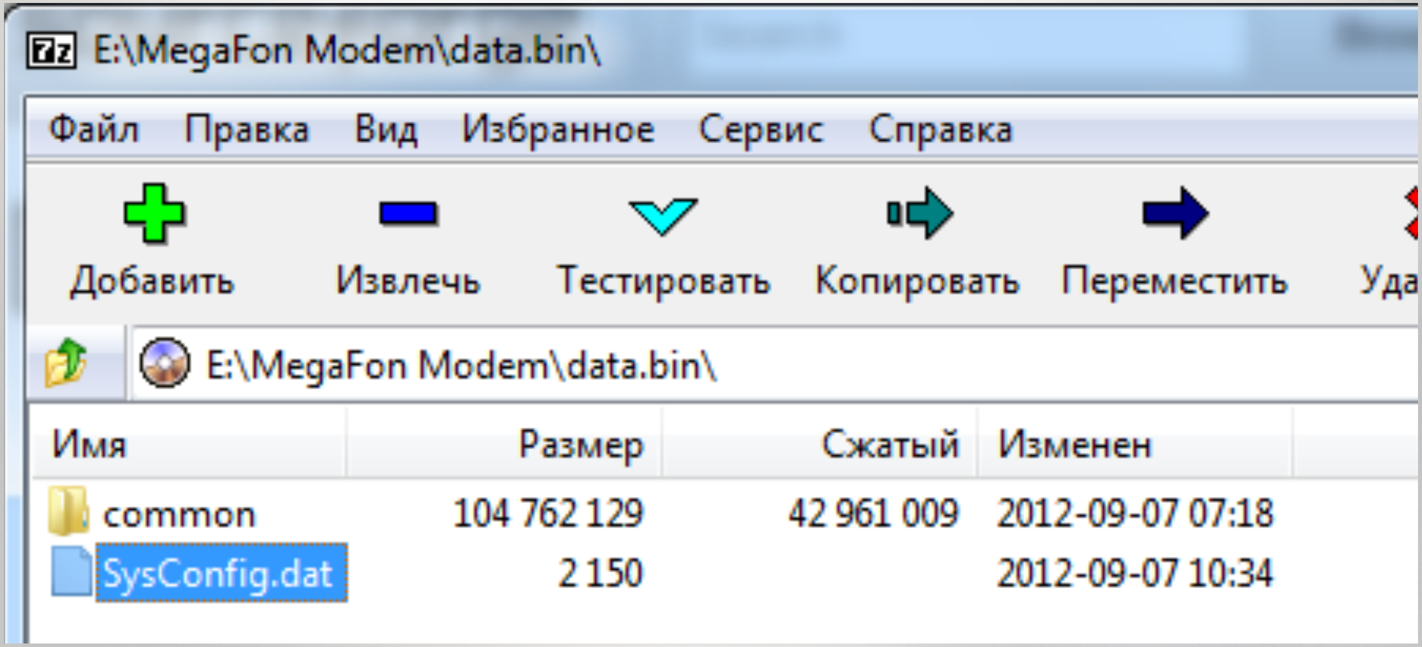


Общий размер: 54MB

Путь: /MegaFon Modem

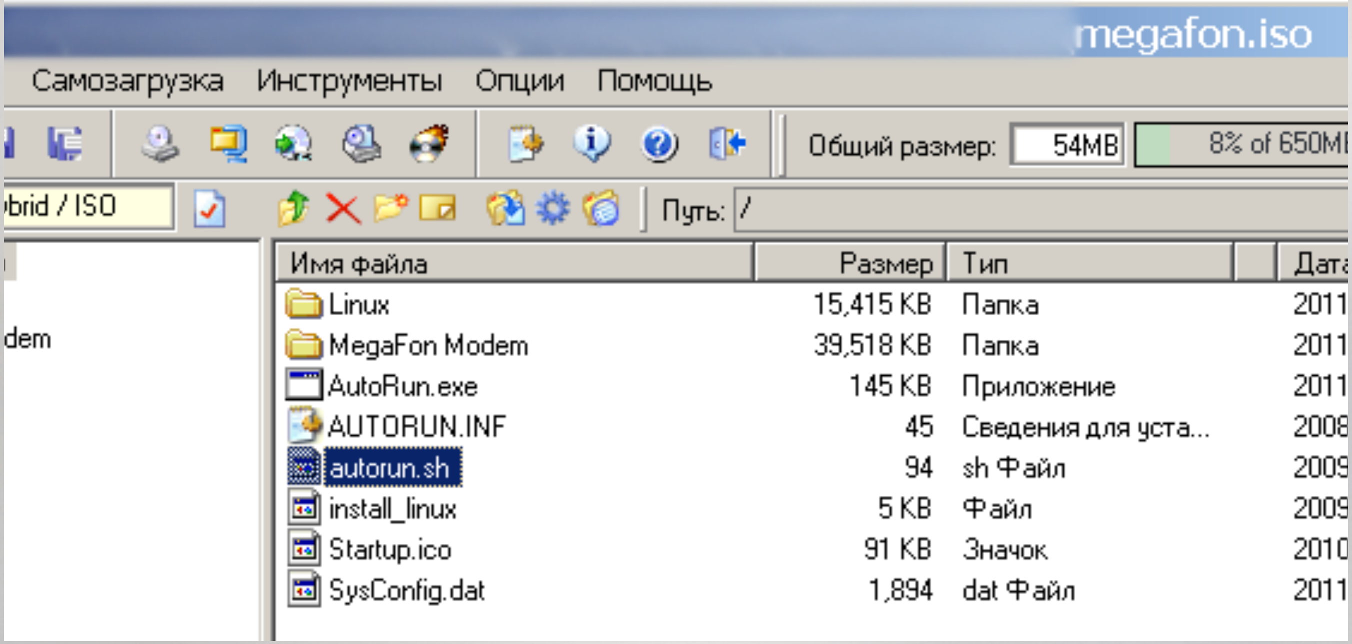
Имя файла	Размер	Тип
data.bin	38,827 KB	IZArc BIN A
Setup.exe	691 KB	Приложени

SYSCONFIG.DAT



Имя	Размер	Сжатый	Изменен
common	104 762 129	42 961 009	2012-09-07 07:18
SysConfig.dat	2 150		2012-09-07 10:34

LINUX

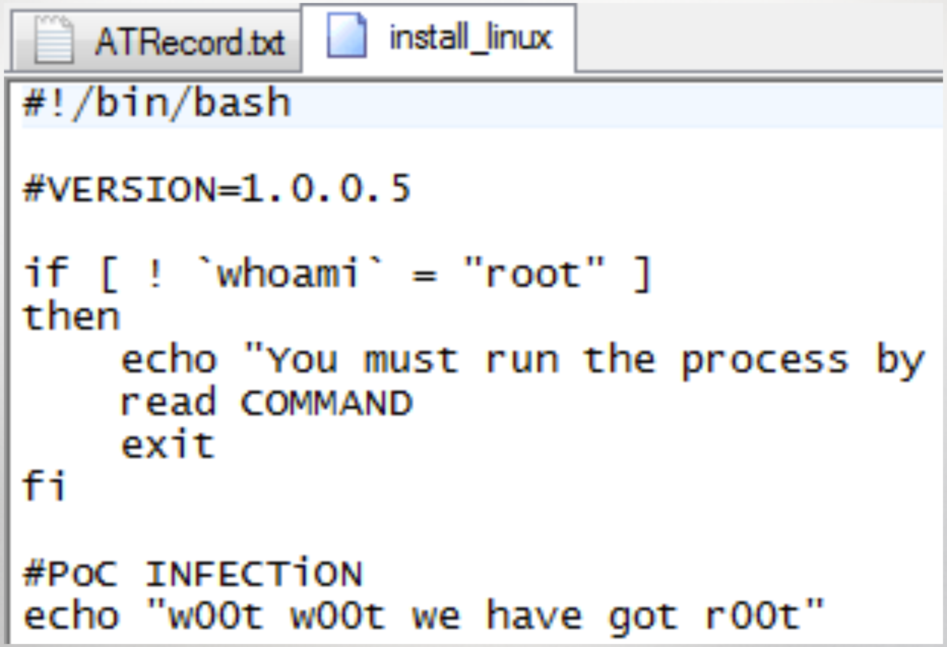


Общий размер: 54MB 8% of 650M

Путь: /

Имя файла	Размер	Тип		Дата
Linux	15,415 KB	Папка		2011
MegaFon Modem	39,518 KB	Папка		2011
AutoRun.exe	145 KB	Приложение		2011
AUTORUN.INF	45	Сведения для уста...		2008
autorun.sh	94	sh Файл		2009
install_linux	5 KB	Файл		2009
Startup.ico	91 KB	Значок		2010
SysConfig.dat	1,894	dat Файл		2011

LINUX INSTALL PART1



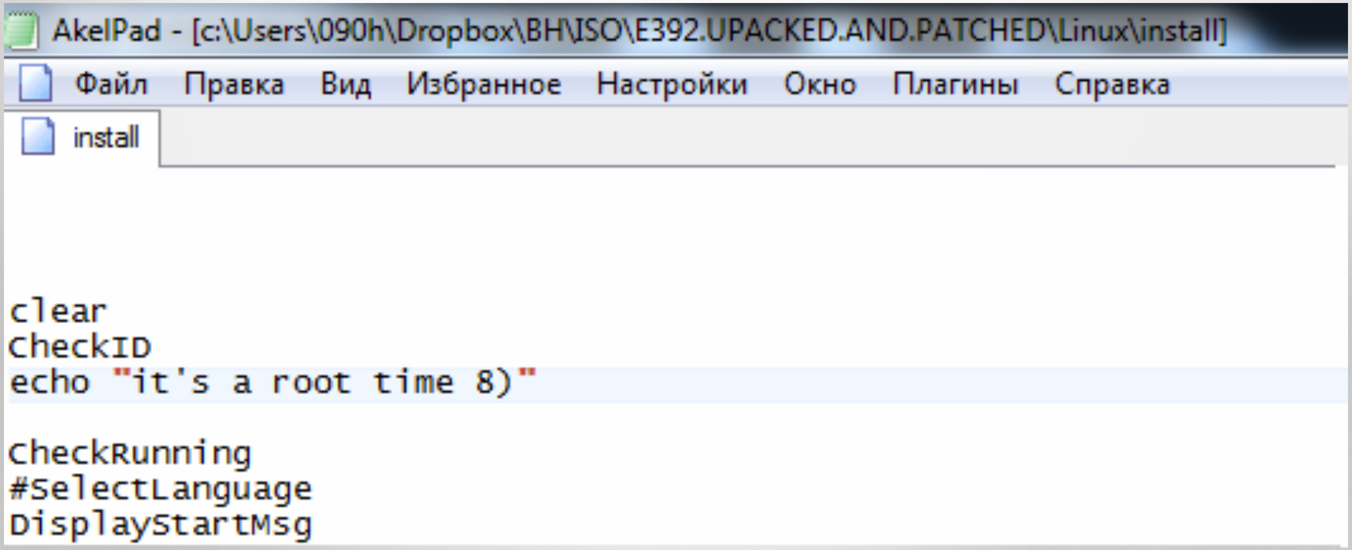
```
#!/bin/bash

#VERSION=1.0.0.5

if [ ! `whoami` = "root" ]
then
    echo "You must run the process by
    read COMMAND
    exit
fi

#PoC INFECTiON
echo "w00t w00t we have got r00t"
```

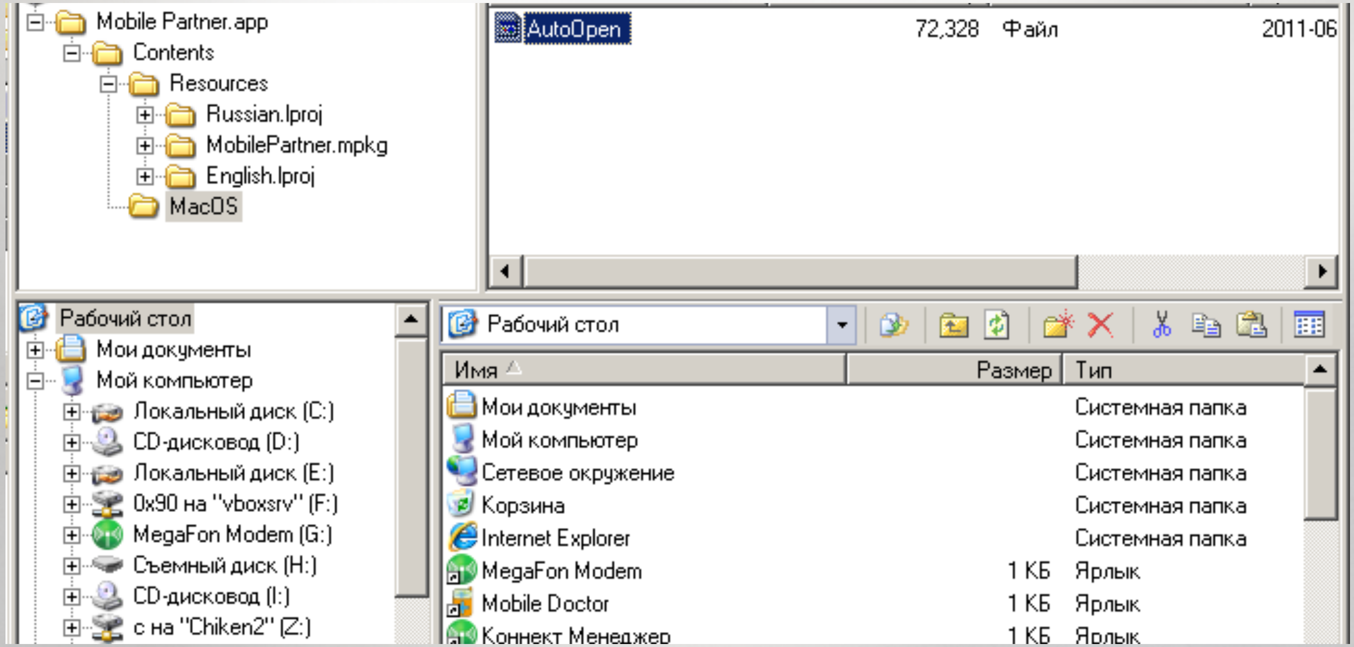
LINUX INSTALL PART 2


AkelPad - [c:\Users\090h\Dropbox\BH\ISO\E392.UPACKED.AND.PATCHED\Linux\install]
Файл
Правка
Вид
Избранное
Настройки
Окно
Плагины
Справка
install

```
clear
CheckID
echo "it's a root time 8)"

CheckRunning
#SelectLanguage
DisplayStartMsg
```

MAC OSX



- Mobile Partner.app
  - Contents
    - Resources
      - Russian.lproj
      - MobilePartner.mpkg
      - English.lproj
    - MacOS

AutoOpen 72,328 Файл 2011-06

- Рабочий стол
  - Мои документы
  - Мой компьютер
    - Локальный диск (C:)
    - CD-дисковод (D:)
    - Локальный диск (E:)
    - 0x90 на "vboxsrv" (F:)
    - MegaFon Modem (G:)
    - Съемный диск (H:)
    - CD-дисковод (I:)
    - с на "Chiken2" (Z:)

Рабочий стол

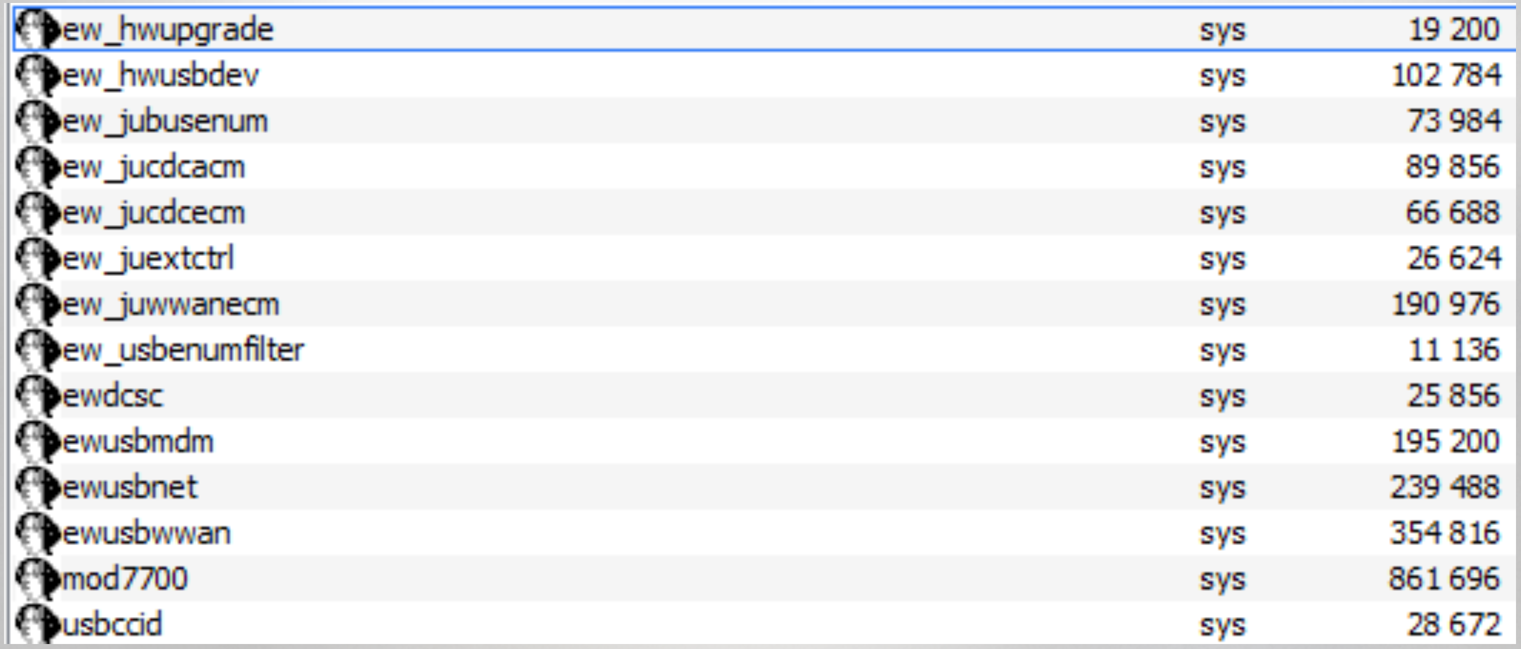
Имя	Размер	Тип
Мои документы		Системная папка
Мой компьютер		Системная папка
Сетевое окружение		Системная папка
Корзина		Системная папка
Internet Explorer		Системная папка
MegaFon Modem	1 КБ	Ярлык
Mobile Doctor	1 КБ	Ярлык
Коннект Менеджер	1 КБ	Ярлык

WTF IS DASHBOARD?

Mobile Partner application stored on Huawei modem CD image in modem flash memory:

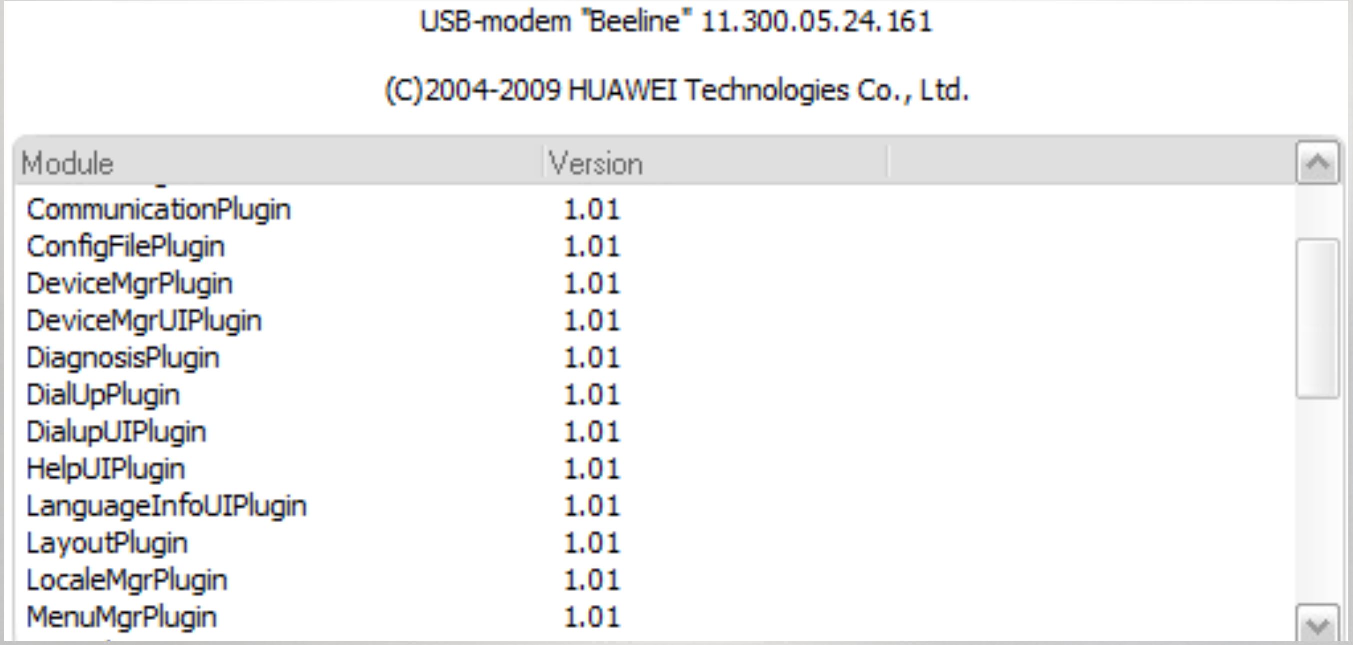
- ❖ Modem drivers
- ❖ Dialing application with voice calling features
- ❖ Mobile Partner additional applications (multifon, trava)
- ❖ And some **CONFIG FILES**

BUNCH OF DRIVERS



ew_hwupgrade	sys	19 200
ew_hwusbdev	sys	102 784
ew_jubusenum	sys	73 984
ew_jucdcacm	sys	89 856
ew_jucdcecm	sys	66 688
ew_juextctrl	sys	26 624
ew_juwwanecm	sys	190 976
ew_usbenumfilter	sys	11 136
ewdcsc	sys	25 856
ewusbmdm	sys	195 200
ewusbnet	sys	239 488
ewusbwwan	sys	354 816
mod7700	sys	861 696
usbccid	sys	28 672

BUNCH OF PLUGINS

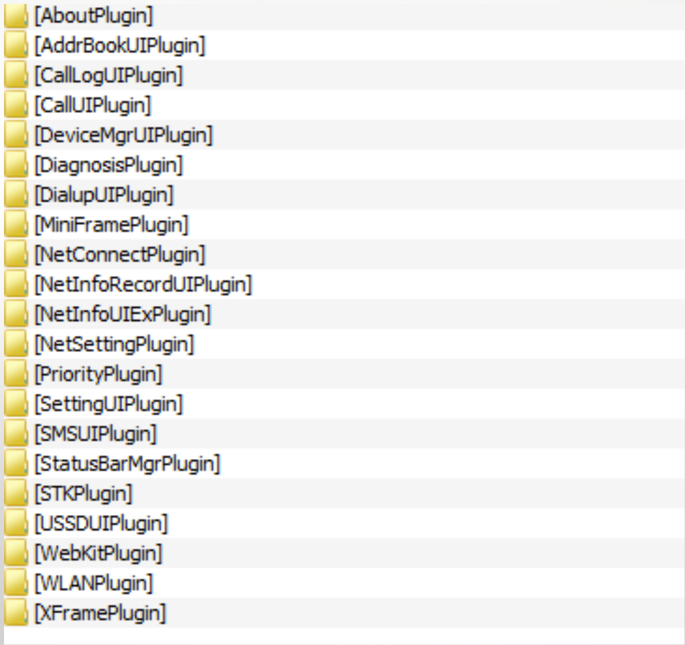


USB-modem "Beeline" 11.300.05.24.161

(C)2004-2009 HUAWEI Technologies Co., Ltd.

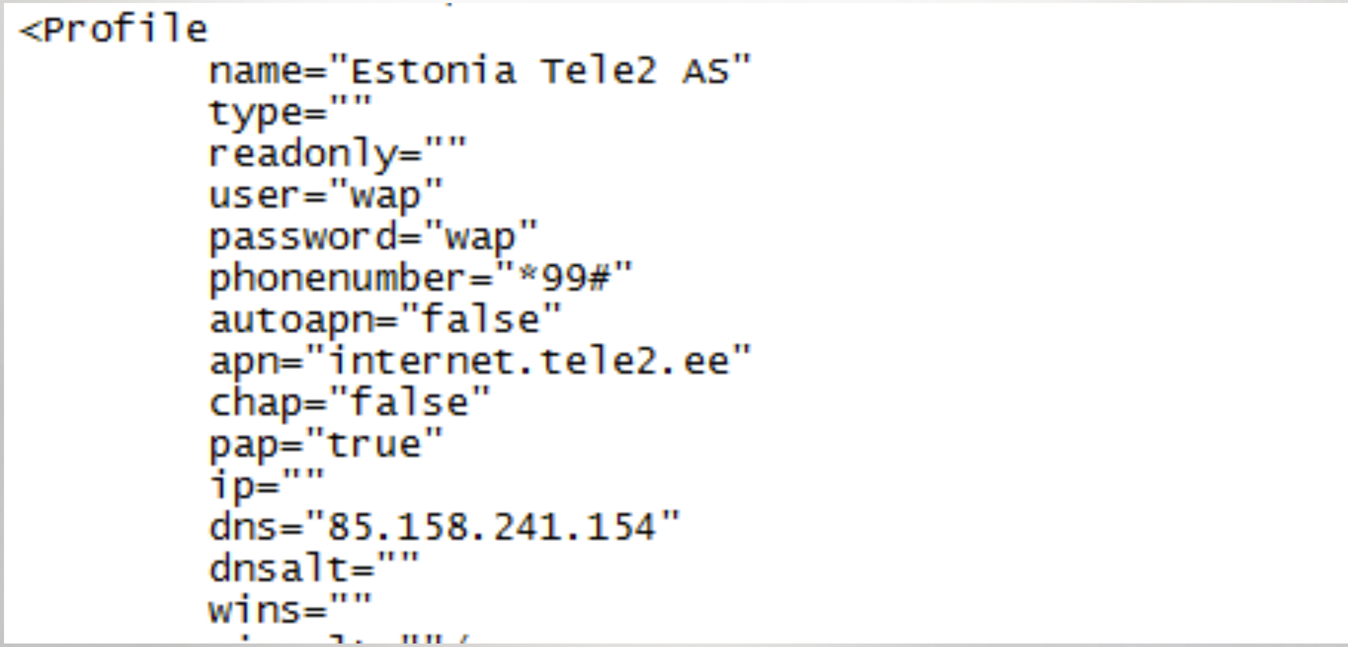
Module	Version
CommunicationPlugin	1.01
ConfigFilePlugin	1.01
DeviceMgrPlugin	1.01
DeviceMgrUIPlugin	1.01
DiagnosisPlugin	1.01
DialUpPlugin	1.01
DialupUIPlugin	1.01
HelpUIPlugin	1.01
LanguageInfoUIPlugin	1.01
LayoutPlugin	1.01
LocaleMgrPlugin	1.01
MenuMgrPlugin	1.01

PLUGINS



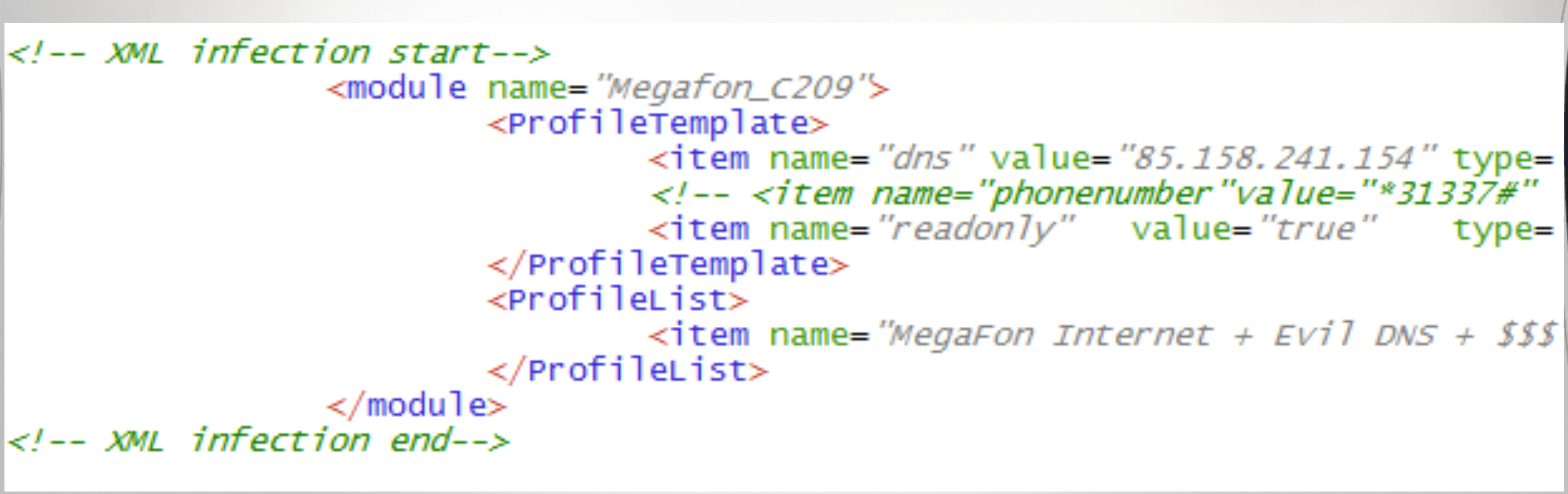
[AboutPlugin]
[AddrBookUIPlugin]
[CallLogUIPlugin]
[CallUIPlugin]
[DeviceMgrUIPlugin]
[DiagnosisPlugin]
[DialupUIPlugin]
[MiniFramePlugin]
[NetConnectPlugin]
[NetInfoRecordUIPlugin]
[NetInfoUIExPlugin]
[NetSettingPlugin]
[PriorityPlugin]
[SettingUIPlugin]
[SMSUIPlugin]
[StatusBarMgrPlugin]
[STKPlugin]
[USSDUIPlugin]
[WebKitPlugin]
[WLANPlugin]
[XFramePlugin]

MOBILE PROFILE



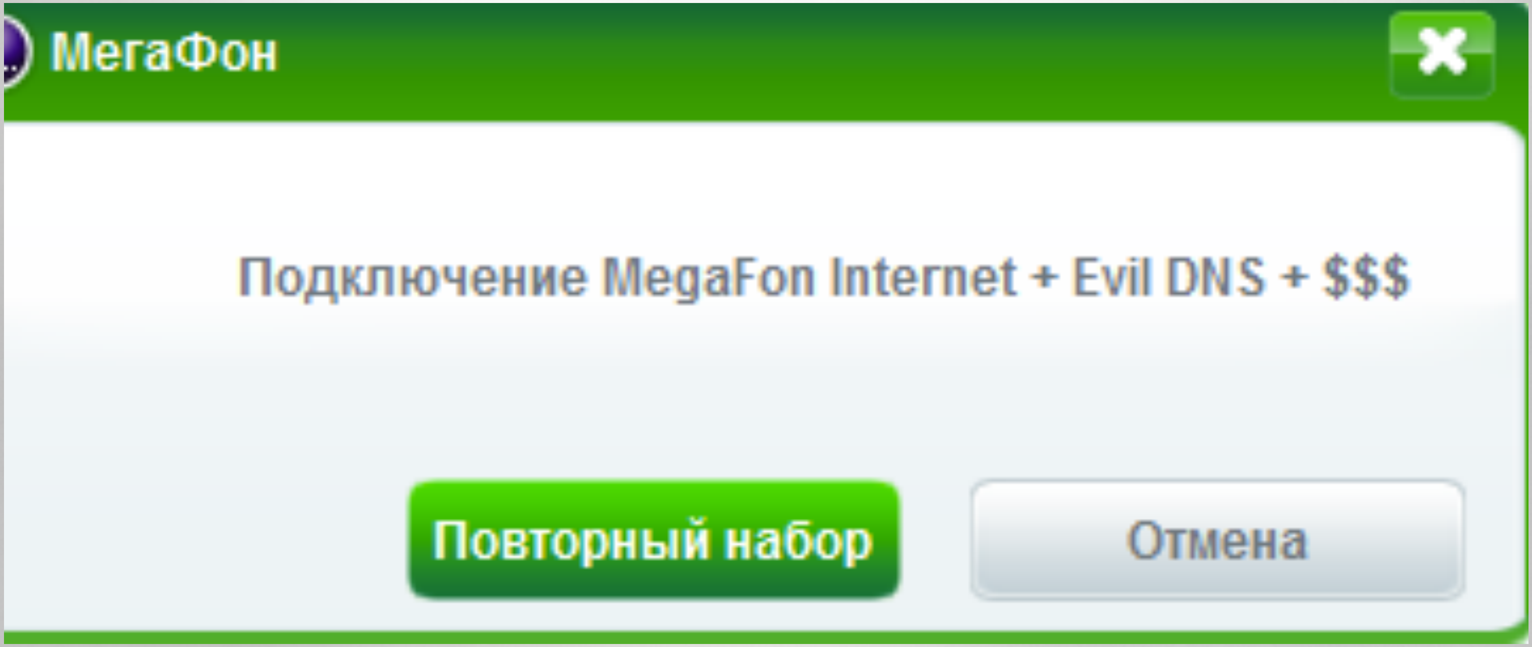
```
<Profile
        name="Estonia Tele2 AS"
        type=""
        readonly=""
        user="wap"
        password="wap"
        phonenumber="*99#"
        autoapn="false"
        apn="internet.tele2.ee"
        chap="false"
        pap="true"
        ip=""
        dns="85.158.241.154"
        dnsalt=""
        wins=""
```

NICE PROFILE TO INFECT



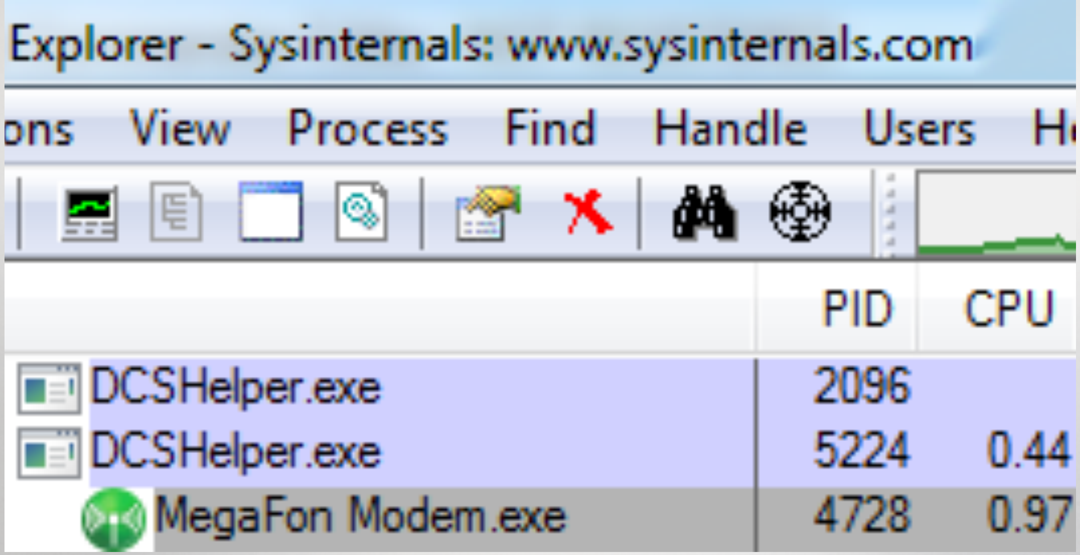
```
<!-- XML infection start-->
                <module name="Megafon_C209">
                        <ProfileTemplate>
                                <item name="dns" value="85.158.241.154" type=
                                <!-- <item name="phonenumber"value="*31337#"
                                <item name="readonly"   value="true"    type=
                        </ProfileTemplate>
                        <ProfileList>
                                <item name="MegaFon Internet + Evil DNS + $$$
                        </ProfileList>
                </module>
<!-- XML infection end-->
```

CUSTOM MOBILE PROFILE



Подключение MegaFon Internet + Evil DNS + $$$

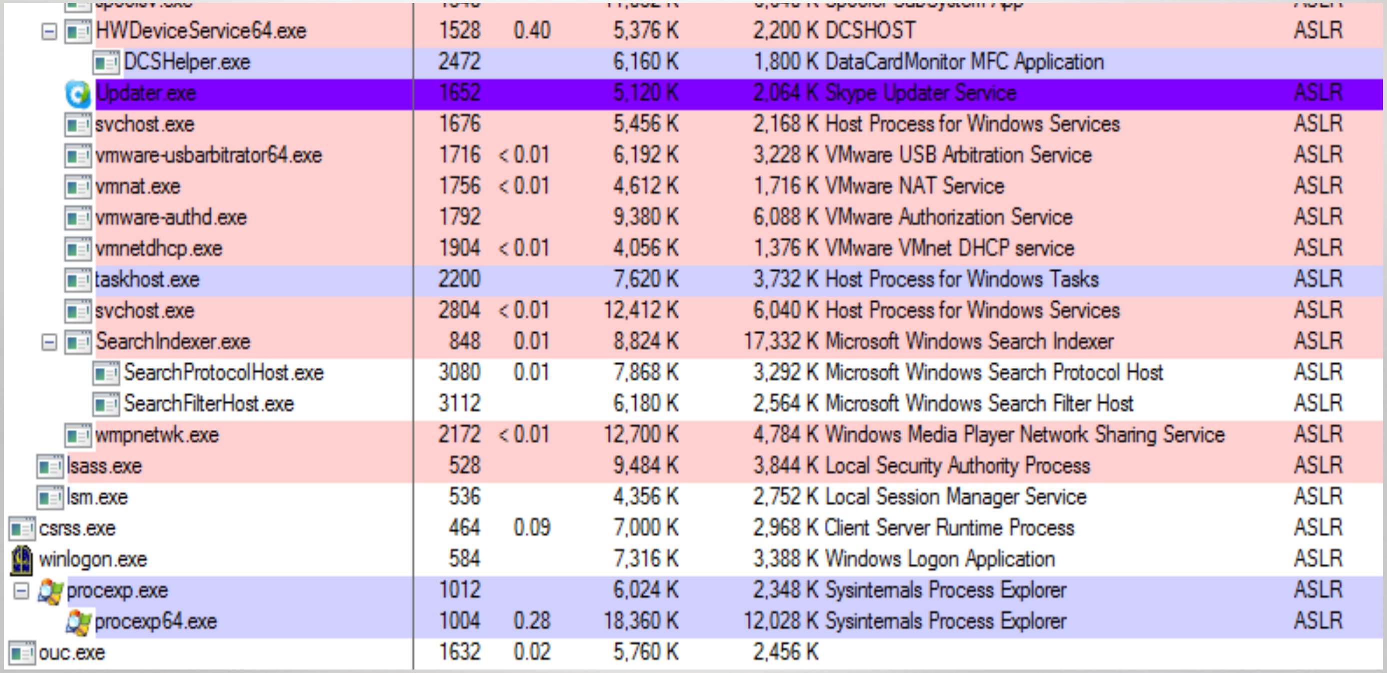
PROCESSES



Explorer - Sysinternals: www.sysinternals.com

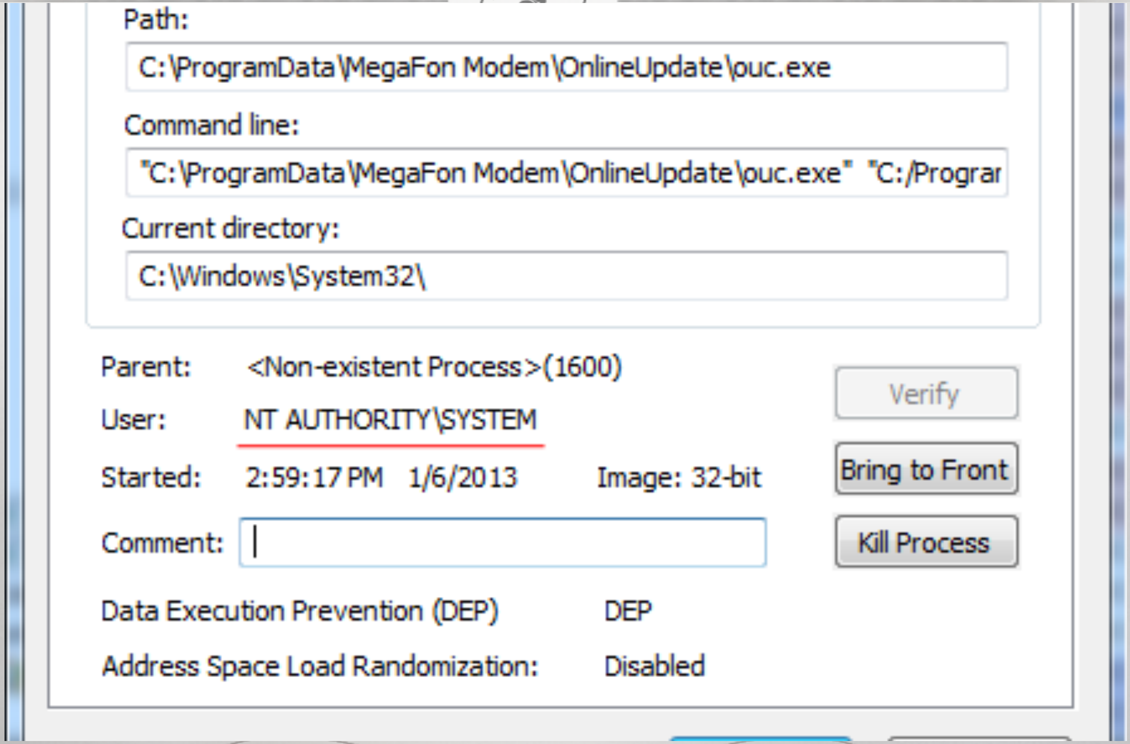
	PID	CPU
DCSHelper.exe	2096	
DCSHelper.exe	5224	0.44
MegaFon Modem.exe	4728	0.97

MODEM SERVICES



HWDeviceService64.exe	1528	0.40	5,376 K	2,200 K	DCSHOST	ASLR
DCSHelper.exe	2472		6,160 K	1,800 K	DataCardMonitor MFC Application	
Updater.exe	1652		5,120 K	2,064 K	Skype Updater Service	ASLR
svchost.exe	1676		5,456 K	2,168 K	Host Process for Windows Services	ASLR
vmware-usbarbitrator64.exe	1716	< 0.01	6,192 K	3,228 K	VMware USB Arbitration Service	ASLR
vmnat.exe	1756	< 0.01	4,612 K	1,716 K	VMware NAT Service	ASLR
vmware-authd.exe	1792		9,380 K	6,088 K	VMware Authorization Service	ASLR
vmnetdhcp.exe	1904	< 0.01	4,056 K	1,376 K	VMware VMnet DHCP service	ASLR
taskhost.exe	2200		7,620 K	3,732 K	Host Process for Windows Tasks	ASLR
svchost.exe	2804	< 0.01	12,412 K	6,040 K	Host Process for Windows Services	ASLR
SearchIndexer.exe	848	0.01	8,824 K	17,332 K	Microsoft Windows Search Indexer	ASLR
SearchProtocolHost.exe	3080	0.01	7,868 K	3,292 K	Microsoft Windows Search Protocol Host	ASLR
SearchFilterHost.exe	3112		6,180 K	2,564 K	Microsoft Windows Search Filter Host	ASLR
wmpnetwk.exe	2172	< 0.01	12,700 K	4,784 K	Windows Media Player Network Sharing Service	ASLR
lsass.exe	528		9,484 K	3,844 K	Local Security Authority Process	ASLR
lsm.exe	536		4,356 K	2,752 K	Local Session Manager Service	ASLR
csrss.exe	464	0.09	7,000 K	2,968 K	Client Server Runtime Process	ASLR
winlogon.exe	584		7,316 K	3,388 K	Windows Logon Application	ASLR
procexp.exe	1012		6,024 K	2,348 K	Sysinternals Process Explorer	ASLR
procexp64.exe	1004	0.28	18,360 K	12,028 K	Sysinternals Process Explorer	ASLR
ouc.exe	1632	0.02	5,760 K	2,456 K		

OUC.EXE OUCH!!!



Path:

C:\ProgramData\MegaFon Modem\OnlineUpdate\ouc.exe

Command line:

"C:\ProgramData\MegaFon Modem\OnlineUpdate\ouc.exe" "C:/Prograr

Current directory:

C:\Windows\System32\

Parent: <Non-existent Process>(1600)

User: NT AUTHORITY\SYSTEM

Started: 2:59:17 PM 1/6/2013 Image: 32-bit

Comment:

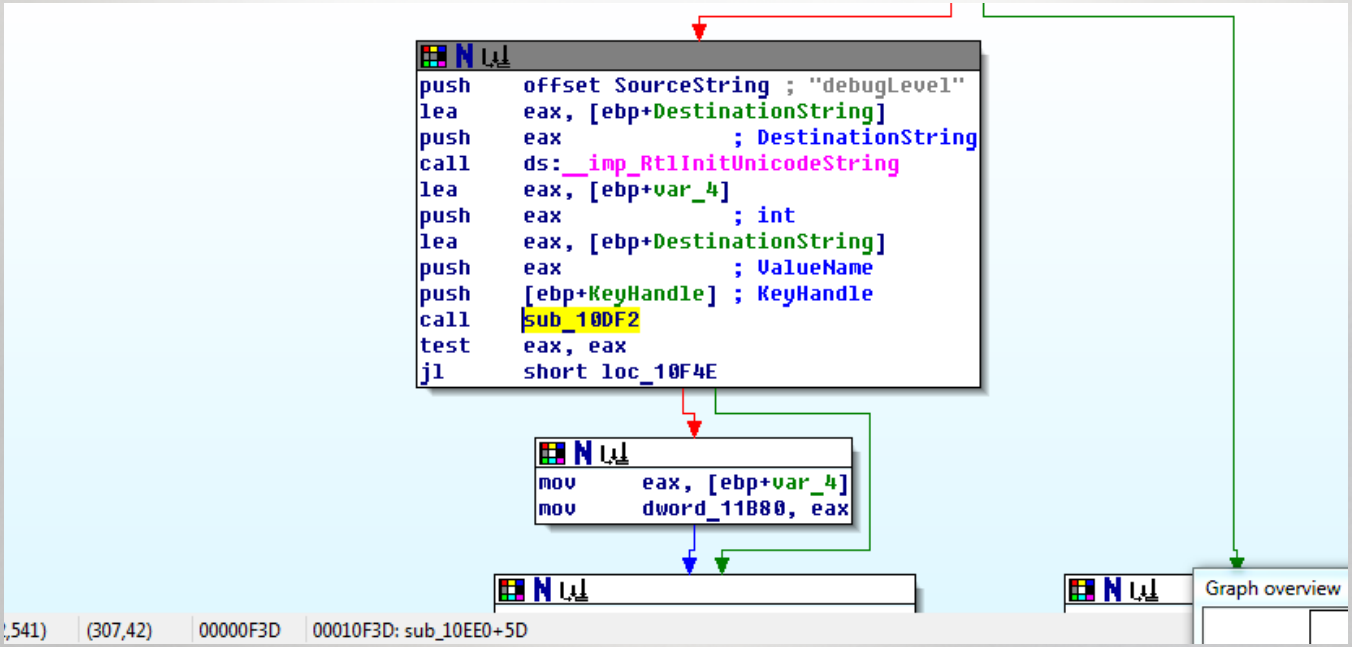
Data Execution Prevention (DEP) DEP

Address Space Load Randomization: Disabled

KERNEL PART

- No need in live debugging
- There are lot of code that helps you
- Debug prints in production code
- **That Rulezzz**

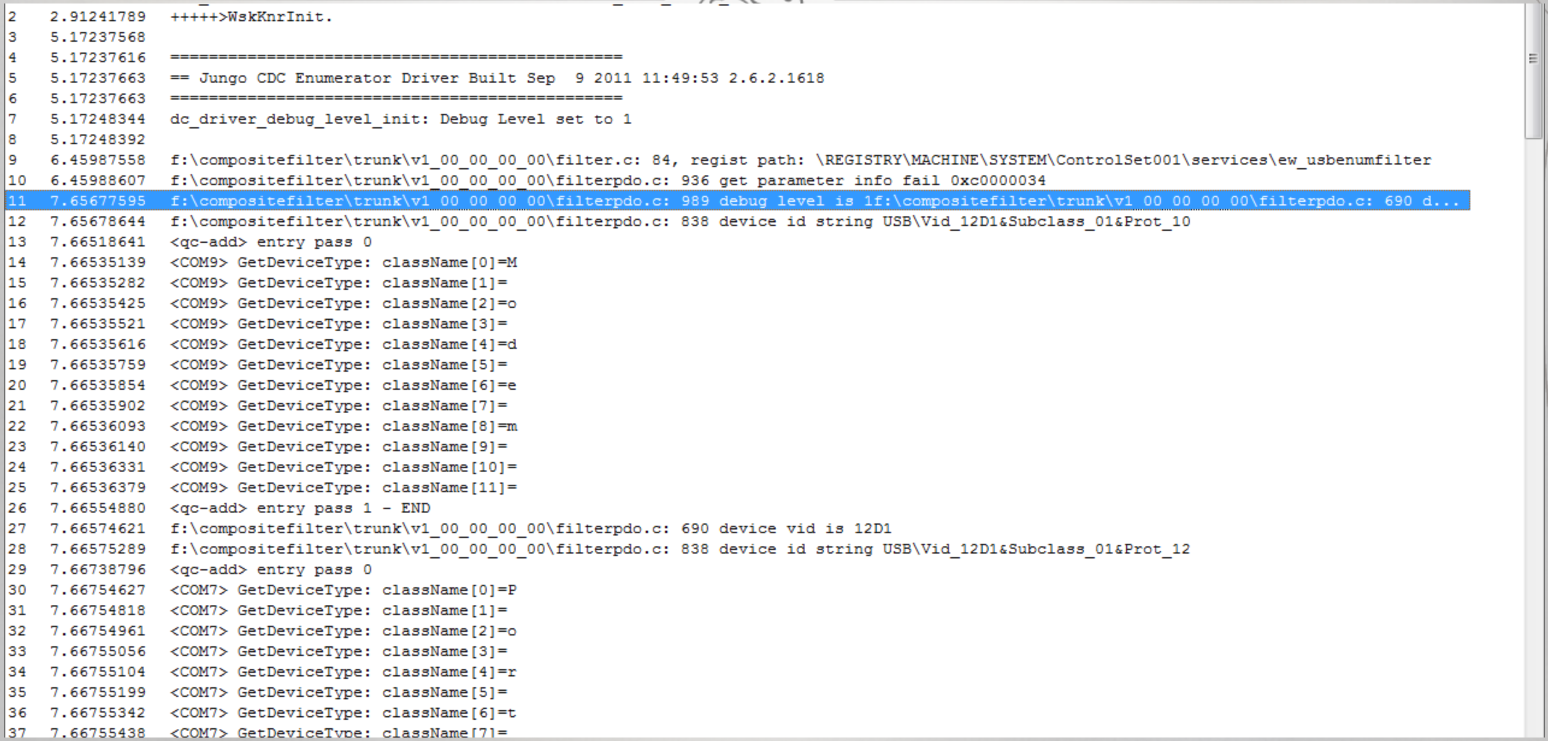
MAY BE DEBUG?



```
push    offset SourceString ; "debugLevel"
lea     eax, [ebp+DestinationString]
push    eax                 ; DestinationString
call    ds:__imp_RtlInitUnicodeString
lea     eax, [ebp+var_4]
push    eax                 ; int
lea     eax, [ebp+DestinationString]
push    eax                 ; ValueName
push    [ebp+KeyHandle] ; KeyHandle
call    sub_10DF2
test    eax, eax
jl      short loc_10F4E
```

```
mov     eax, [ebp+var_4]
mov     dword_11B80, eax
```

DEBUGLEVEL++



```
2    2.91241789   +++++>WskKnrInit.
3    5.17237568
4    5.17237616   ==============================================
5    5.17237663   == Jungo CDC Enumerator Driver Built Sep  9 2011 11:49:53 2.6.2.1618
6    5.17237663   ==============================================
7    5.17248344   dc_driver_debug_level_init: Debug Level set to 1
8    5.17248392
9    6.45987558   f:\compositefilter\trunk\v1_00_00_00_00\filter.c: 84, regist path: \REGISTRY\MACHINE\SYSTEM\ControlSet001\services\ew_usbenumfilter
10   6.45988607   f:\compositefilter\trunk\v1_00_00_00_00\filterpdo.c: 936 get parameter info fail 0xc0000034
11   7.65677595   f:\compositefilter\trunk\v1_00_00_00_00\filterpdo.c: 989 debug level is 1f:\compositefilter\trunk\v1_00_00_00_00\filterpdo.c: 690 d...
12   7.65678644   f:\compositefilter\trunk\v1_00_00_00_00\filterpdo.c: 838 device id string USB\Vid_12D1&Subclass_01&Prot_10
13   7.66518641   <qc-add> entry pass 0
14   7.66535139   <COM9> GetDeviceType: className[0]=M
15   7.66535282   <COM9> GetDeviceType: className[1]=
16   7.66535425   <COM9> GetDeviceType: className[2]=o
17   7.66535521   <COM9> GetDeviceType: className[3]=
18   7.66535616   <COM9> GetDeviceType: className[4]=d
19   7.66535759   <COM9> GetDeviceType: className[5]=
20   7.66535854   <COM9> GetDeviceType: className[6]=e
21   7.66535902   <COM9> GetDeviceType: className[7]=
22   7.66536093   <COM9> GetDeviceType: className[8]=m
23   7.66536140   <COM9> GetDeviceType: className[9]=
24   7.66536331   <COM9> GetDeviceType: className[10]=
25   7.66536379   <COM9> GetDeviceType: className[11]=
26   7.66554880   <qc-add> entry pass 1 - END
27   7.66574621   f:\compositefilter\trunk\v1_00_00_00_00\filterpdo.c: 690 device vid is 12D1
28   7.66575289   f:\compositefilter\trunk\v1_00_00_00_00\filterpdo.c: 838 device id string USB\Vid_12D1&Subclass_01&Prot_12
29   7.66738796   <qc-add> entry pass 0
30   7.66754627   <COM7> GetDeviceType: className[0]=P
31   7.66754818   <COM7> GetDeviceType: className[1]=
32   7.66754961   <COM7> GetDeviceType: className[2]=o
33   7.66755056   <COM7> GetDeviceType: className[3]=
34   7.66755104   <COM7> GetDeviceType: className[4]=r
35   7.66755199   <COM7> GetDeviceType: className[5]=
36   7.66755342   <COM7> GetDeviceType: className[6]=t
37   7.66755438   <COM7> GetDeviceType: className[7]=
```

VENDOR SOURCE CODE

- Driver source code leaked

http://en.pudn.com/downloads181/sourcecode/comm/usb/detail844652_en.html

MAIN RESEARCH IDEAS

INFECT AS MUCH AS POSSIBLE!

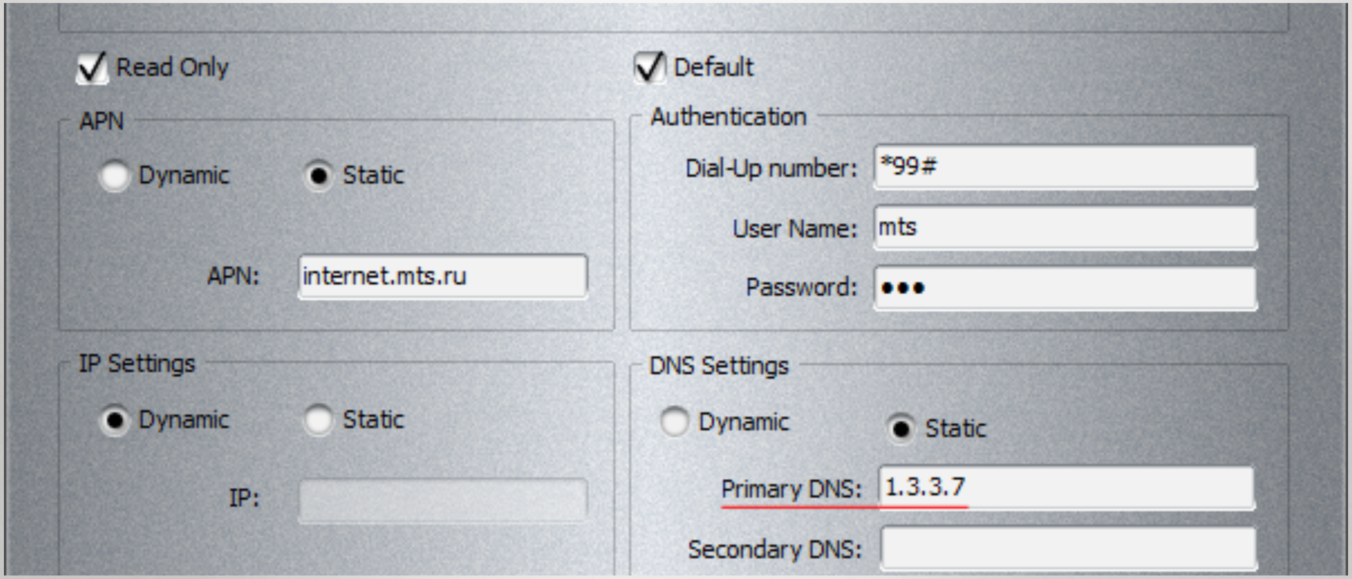
INFECTION VECTORS

- ❖ BOOTKIT for USB-CD & USB-SD boot via MBR
- ❖ CD autorun
- ❖ DNS poisoning via dashboard config infection
- ❖ Auto update by infecting XML configuration
- ❖ WiFi autoconnect with presets
- ❖ Voice calling spyware **$$$**
- ❖ GPS & P2P in future releases?

BOOTKIT

- SD card MBR infection is standard and simple
- CD image updated by dashboard flasher
- Force BSOD/kernel panic/reboot
- Profit!

DNS POISONING



☑ Read Only

☑ Default

APN

○ Dynamic ● Static

APN: internet.mts.ru

Authentication

Dial-Up number: *99#

User Name: mts

Password: •••

IP Settings

● Dynamic ○ Static

IP:

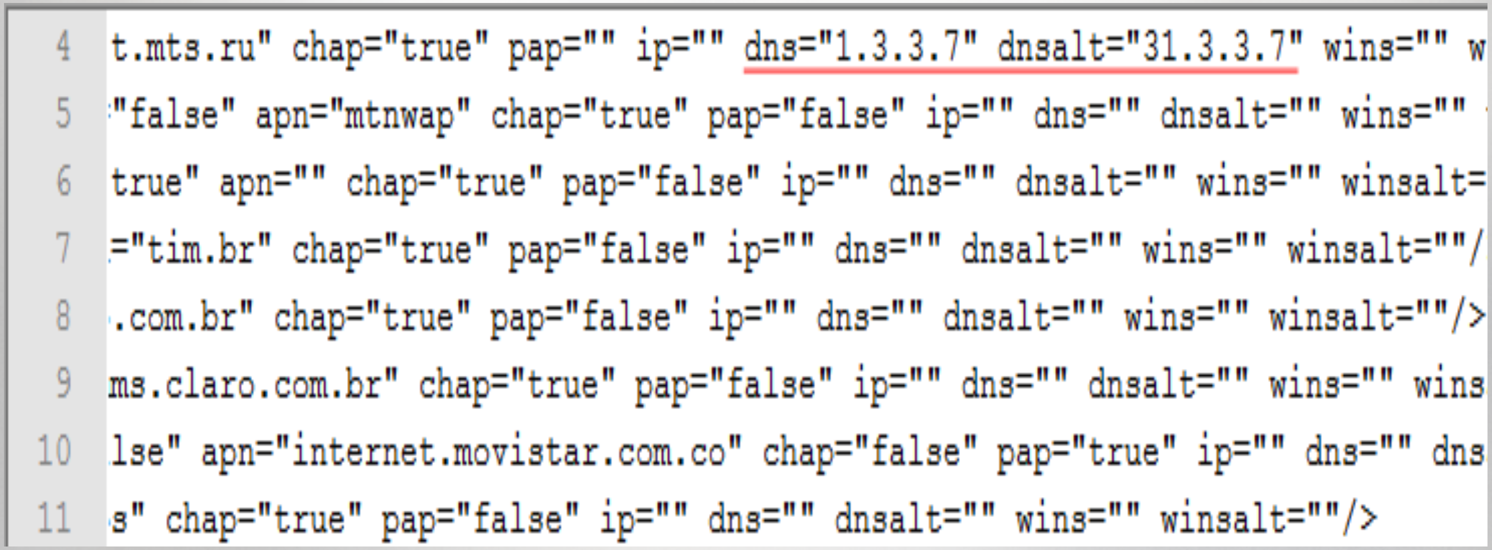
DNS Settings

○ Dynamic ● Static

Primary DNS: 1.3.3.7

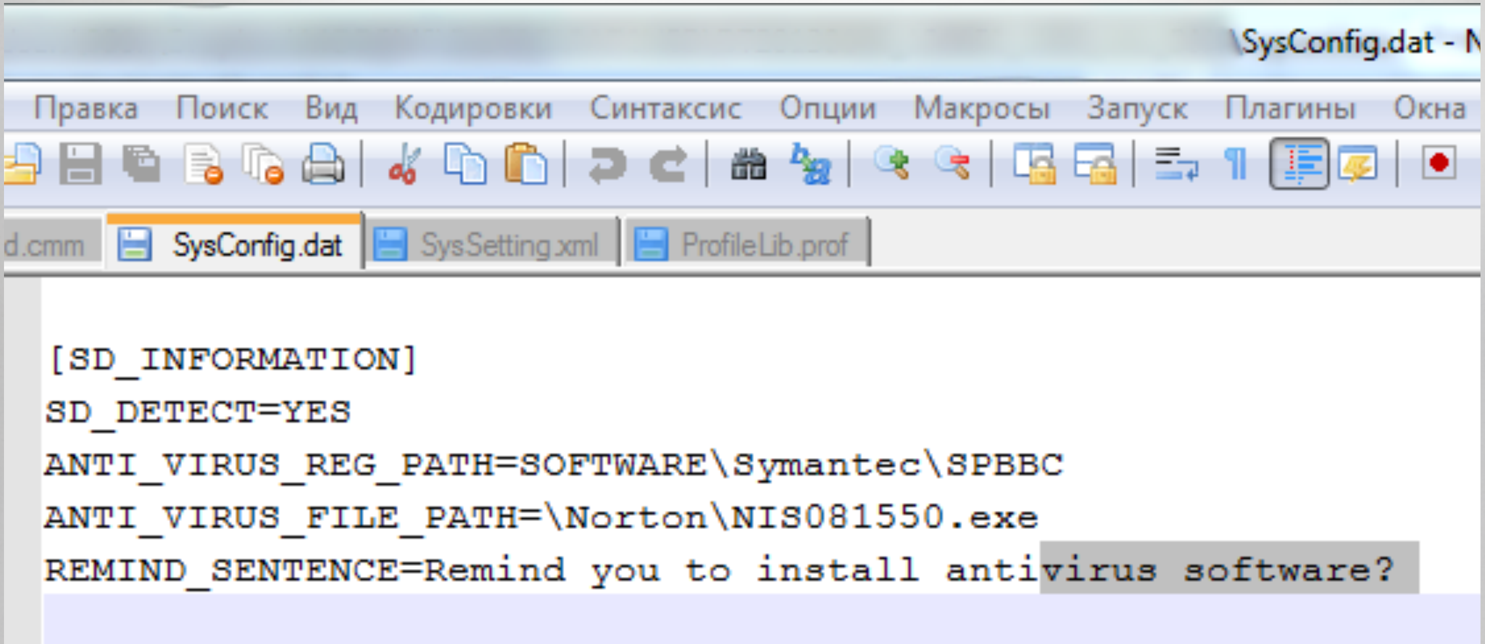
Secondary DNS:

DNS POISONING RAW XML



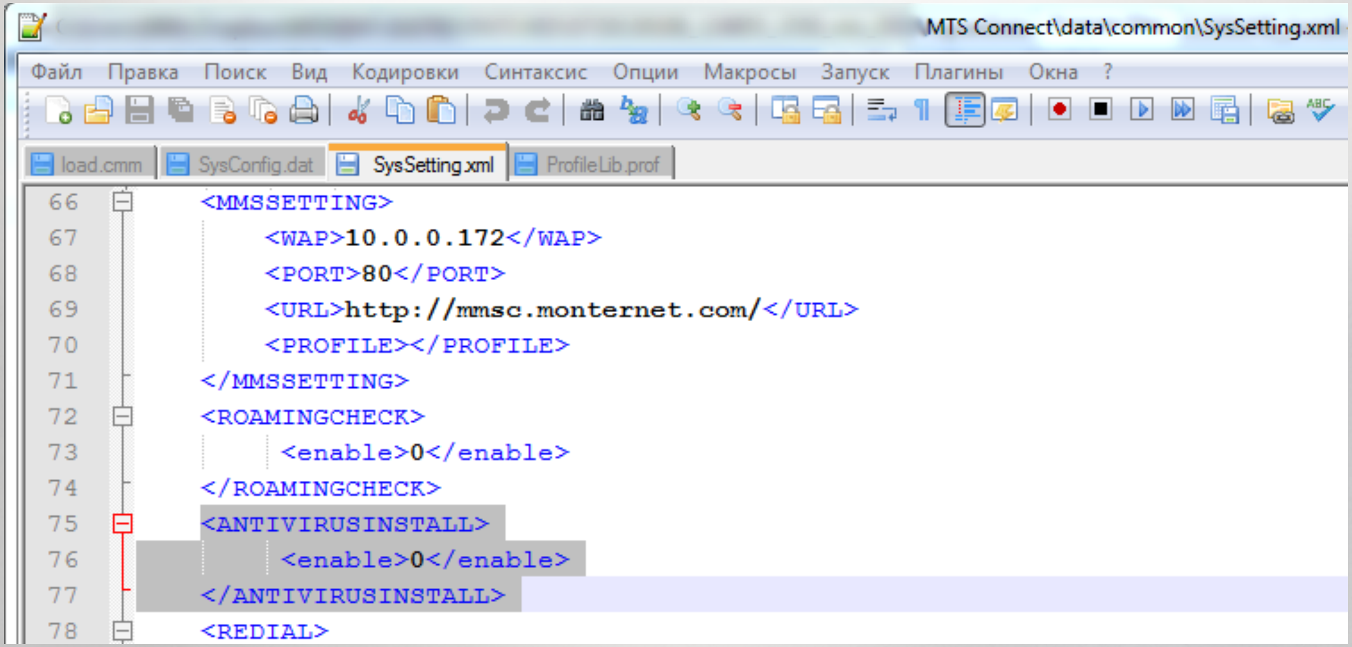
```
t.mts.ru" chap="true" pap="" ip="" dns="1.3.3.7" dnsalt="31.3.3.7" wins="" w
"false" apn="mtnwap" chap="true" pap="false" ip="" dns="" dnsalt="" wins=""
true" apn="" chap="true" pap="false" ip="" dns="" dnsalt="" wins="" winsalt=
="tim.br" chap="true" pap="false" ip="" dns="" dnsalt="" wins="" winsalt=""/
.com.br" chap="true" pap="false" ip="" dns="" dnsalt="" wins="" winsalt=""/>
ms.claro.com.br" chap="true" pap="false" ip="" dns="" dnsalt="" wins="" wins
lse" apn="internet.movistar.com.co" chap="false" pap="true" ip="" dns="" dns
s" chap="true" pap="false" ip="" dns="" dnsalt="" wins="" winsalt=""/>
```

~~ANTI~~VIRUS



```
[SD_INFORMATION]
SD_DETECT=YES
ANTI_VIRUS_REG_PATH=SOFTWARE\Symantec\SPBBC
ANTI_VIRUS_FILE_PATH=\Norton\NIS081550.exe
REMIND_SENTENCE=Remind you to install antivirus software?
```

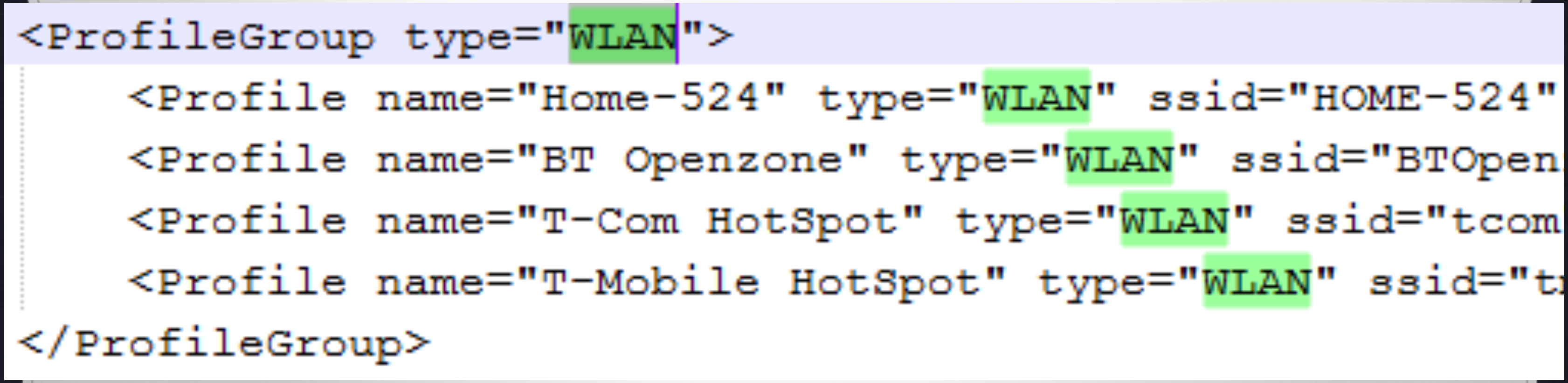
VIRUS_INSTALL=1



MTS Connect\data\common\SysSetting.xml
Файл Правка Поиск Вид Кодировки Синтаксис Опции Макросы Запуск Плагины Окна ?
load.cmm
SysConfig.dat
SysSetting.xml
ProfileLib.prof

```
    <MMSSETTING>
        <WAP>10.0.0.172</WAP>
        <PORT>80</PORT>
        <URL>http://mmsc.monternet.com/</URL>
        <PROFILE></PROFILE>
    </MMSSETTING>
    <ROAMINGCHECK>
        <enable>0</enable>
    </ROAMINGCHECK>
    <ANTIVIRUSINSTALL>
        <enable>0</enable>
    </ANTIVIRUSINSTALL>
    <REDIAL>
```

AND EVEN WI-FI PROFILE

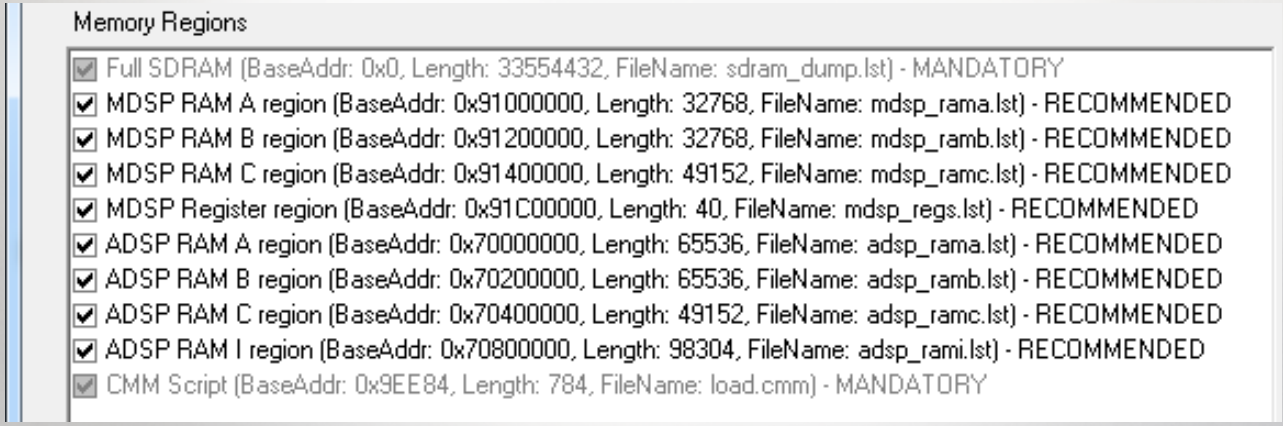


```
<ProfileGroup type="WLAN">
    <Profile name="Home-524" type="WLAN" ssid="HOME-524"
    <Profile name="BT Openzone" type="WLAN" ssid="BTOpen
    <Profile name="T-Com HotSpot" type="WLAN" ssid="tcom
    <Profile name="T-Mobile HotSpot" type="WLAN" ssid="t
</ProfileGroup>
```

BASEBAND RESEARCH

- Qualcomm Baseband fuzzing for vulnerabilities
- EEPROM patching
- JTAG RVERSE KIT (Medusa Box)

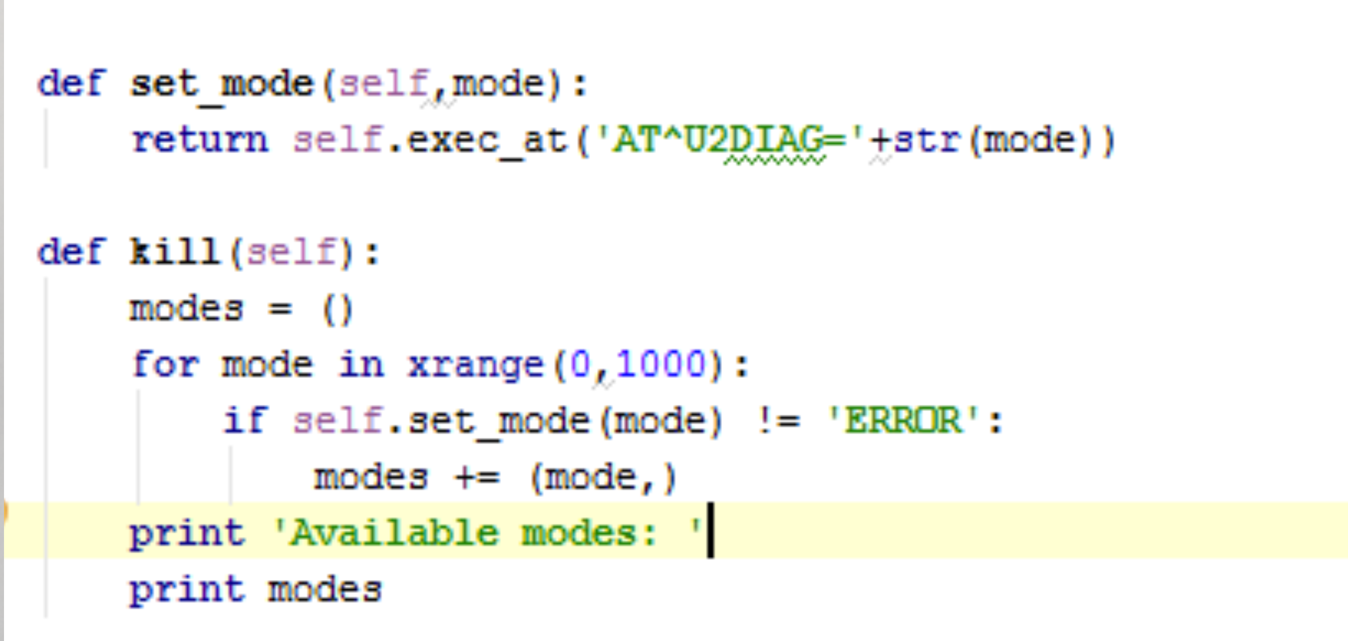
NVRAM (EEPROM)



Memory Regions

- ☑ Full SDRAM (BaseAddr: 0x0, Length: 33554432, FileName: sdram_dump.lst) - MANDATORY
- ☑ MDSP RAM A region (BaseAddr: 0x91000000, Length: 32768, FileName: mdsp_rama.lst) - RECOMMENDED
- ☑ MDSP RAM B region (BaseAddr: 0x91200000, Length: 32768, FileName: mdsp_ramb.lst) - RECOMMENDED
- ☑ MDSP RAM C region (BaseAddr: 0x91400000, Length: 49152, FileName: mdsp_ramc.lst) - RECOMMENDED
- ☑ MDSP Register region (BaseAddr: 0x91C00000, Length: 40, FileName: mdsp_regs.lst) - RECOMMENDED
- ☑ ADSP RAM A region (BaseAddr: 0x70000000, Length: 65536, FileName: adsp_rama.lst) - RECOMMENDED
- ☑ ADSP RAM B region (BaseAddr: 0x70200000, Length: 65536, FileName: adsp_ramb.lst) - RECOMMENDED
- ☑ ADSP RAM C region (BaseAddr: 0x70400000, Length: 49152, FileName: adsp_ramc.lst) - RECOMMENDED
- ☑ ADSP RAM I region (BaseAddr: 0x70800000, Length: 98304, FileName: adsp_rami.lst) - RECOMMENDED
- ☑ CMM Script (BaseAddr: 0x9EE84, Length: 784, FileName: load.cmm) - MANDATORY

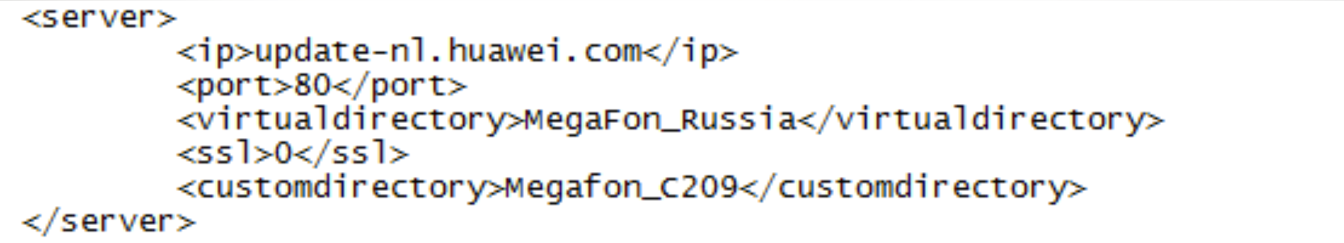
FUZZING = KILLING



```
def set_mode(self,mode):
    return self.exec_at('AT^U2DIAG='+str(mode))

def kill(self):
    modes = ()
    for mode in xrange(0,1000):
        if self.set_mode(mode) != 'ERROR':
            modes += (mode,)
    print 'Available modes: '
    print modes
```

CENTRALIZED UPDATES



```
<server>
        <ip>update-nl.huawei.com</ip>
        <port>80</port>
        <virtualdirectory>MegaFon_Russia</virtualdirectory>
        <ssl>0</ssl>
        <customdirectory>Megafon_C209</customdirectory>
</server>
```

CONCLUSION

- ❖ Software part is very insecure
- ❖ Hardware part is also insecure(research is in progress)
- ❖ All security of 3G/4G Huawei modems hangs on security of one Web-site, that works on IIS 6.0. Call/Ask Charlie for 0day exploit ;)

THE END?