# Symbian worm Yxes: Towards mobile botnets ?

Axelle Apvrille, Fortinet

May 10, 2010

# What is this Presentation about?

## Hesitating to attend?

That's what the talk is about:

- Reverse engineering of a famous malware for mobile phones
- First encountered in 2009, still active in 2010
- Major findings:
  - Decryption of malicious URLs
  - Silent installation of malware
- Contains ARM Assembly code, but don't worry, explained!
- Additional details included in the paper

EICAR 2010

**Presenting SymbOS/Yxes**

Global Overview

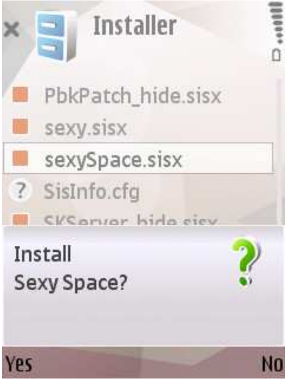
Finding URLs of Remote Servers

Communication with Remote Servers

Silent Installation

Proof or Guess?

# The Symbian Yxes Worm



Installer

PbkPatch_hide.sisx

sexy.sisx

sexySpace.sisx

SisInfo.cfg

SKServer_hide.sisx

Install Sexy Space?

## What is it?

A **worm** for mobile phones. It sends SMS and connects to Internet.

## Is it important?

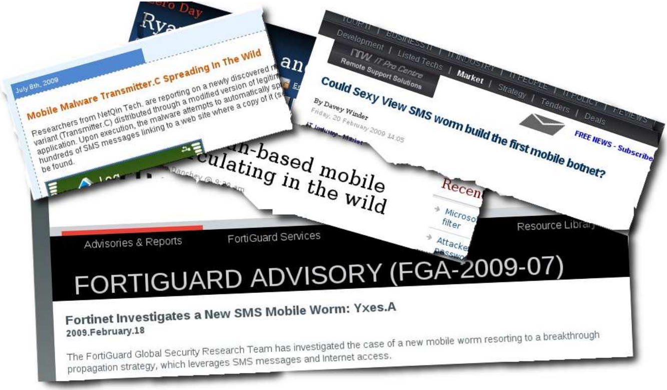
1. High bills for victims
2. Targets Symbian OS 9 - Estimated market share $>$ 15% ($\approx$ 50% for Symbian OS)
3. *"Hundreds of thousands"* devices in China [source: Daniel Hoffman, CTO of Smobile]

## The name

Malicious application's name, Sexy, reversed = Yxes - *Aliases*: SymbOS.Exy, Yxe ...

# SymbOS/Yxes in the IT press

- High bills for victims
- First malware for Symbian OS 9
- Ability to connect to Internet
- Is it a botnet ?



Zero Day

Rya

an

July 8th, 2009

Mobile Malware Transmitter.C Spreading In The Wild

Researchers from NetQin Tech. are reporting on a newly discovered m
variant (Transmitter.C) distributed through a modified version of legitim
application. Upon execution, the malware attempts to automatically sp
hundreds of SMS messages linking to a web site where a copy of it (s
be found.

YOUR IT | BUSINESS IT | IT INDUSTRY | IT PEOPLE | IT POLICY | REVIEWS

Development | Listed Techs | Market | Strategy | Tenders | Deals

ITPW IT Pro Centre
Remote Support Solutions

Could Sexy View SMS worm build the first mobile botnet?

By Davey Winder
Friday, 20 February 2009 14:05
IT Industry - Market

FREE NEWS - Subscribe

an-based mobile
culating in the wild

Danchey @ 9:28 am

Recen

Microso
filter

Attacke
passwo

Advisories & Reports    FortiGuard Services    Resource Library

FORTIGUARD ADVISORY (FGA-2009-07)

Fortinet Investigates a New SMS Mobile Worm: Yxes.A

2009.February.18

The FortiGuard Global Security Research Team has investigated the case of a new mobile worm resorting to a breakthrough propagation strategy, which leverages SMS messages and Internet access.

# SymbOS/Yxes is Signed!

SymbOS/Yxes bears a valid signature, with capabilities:

- Read user's contacts = ReadUserData (basic)
- Send SMS, connect to Internet = NetworkServices (basic)
- Kill applications = PowerMgmt (extended)
- Get the IMEI, IMSI = ReadDeviceData (extended)

## Symbian Signed Programs

Self Signed, Open Signed Online **insufficient**: capability / IMEI restrictions.
Extended capabilities → **Express Signed**
Apply for a PublisherID (from TC TrustCenter)

## Defeating Express Signed

Apply for a PublisherID under a fake identity (or hack a legitimate Express Signed account ?) GUESS
Only costs 20 USD: *affordable*

Presenting SymbOS/Yxes

**Global Overview**

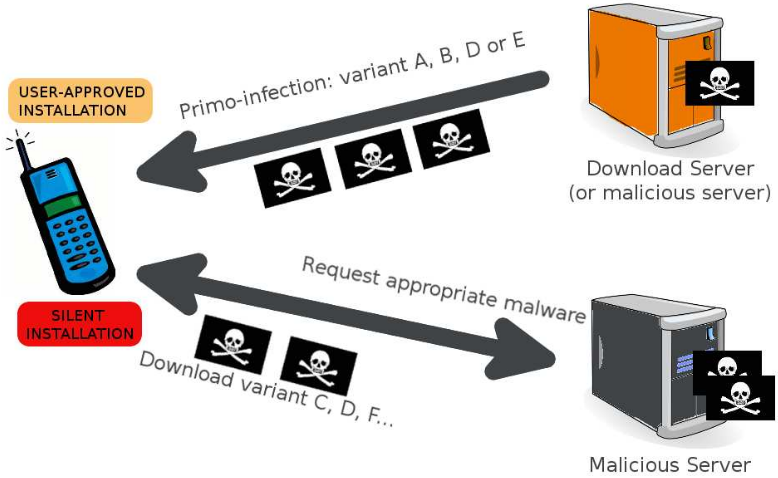
Finding URLs of Remote Servers

Communication with Remote Servers

Silent Installation

Proof or Guess?

# Infection



USER-APPROVED INSTALLATION

Primo-infection: variant A, B, D or E

Download Server (or malicious server)

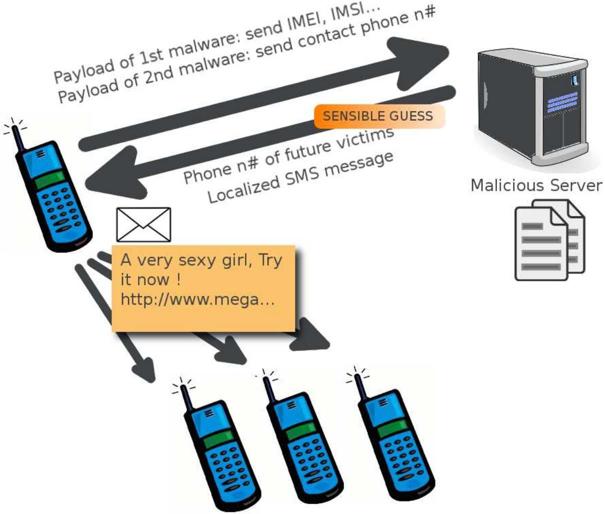
SILENT INSTALLATION

Request appropriate malware

Download variant C, D, F...

Malicious Server

# Payload and Propagation



Payload of 1st malware: send IMEI, IMSI...
Payload of 2nd malware: send contact phone n#

SENSIBLE GUESS

Phone n# of future victims
Localized SMS message

Malicious Server

A very sexy girl, Try it now !
http://www.mega...

Presenting SymbOS/Yxes

Global Overview

**Finding URLs of Remote Servers**

Communication with Remote Servers

Silent Installation

Proof or Guess?

# Strings in the Malicious Executable

### Uncompress the malware

```
$ wine petran.exe -nocompress YxesMalware.exe
PETRAN - PE file preprocessor V02.01 (Build 576)
Copyright (c) 1996-2007 Symbian Software Ltd.
```

### No domain name in the strings !

```
$ strings YxesMalware.exe
Jump.jsp?Version=
Kernel.jsp?Version=
KernelPara.jsp?Version=
...
$ strings –encoding=l YxesMalware.exe
... (no URL) ...
```

# Building URLs in the Code

### Assembly code in SymbOS/Yxes.E!worm

```
SUB     R0, R11, #0x8C ; temporary buffer
LDR     R1, =aKernel_jspVers ; "Kernel.jsp?Version="
BL      _ZN6TPtrC8C1EPKh ; TPtrC8::TPtrC8(uchar  const*)
SUB     R3, R11, #0x8C
SUB     R0, R11, #0x74
MOV   R1, R3
; TDes8::Append(TDesC8  const&)
BL      _ZN5TDes86AppendERK6TDesC8
```

→ R11 - 0x74 holds the beginning of the URL. **Where is the domain name?**

→ R11 - 0x8C holds the end of URL. Appended to beginning.

# Hunting Domain Names

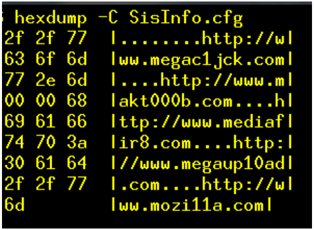
The domain names are read from c:\system\data\SisInfo.cfg

Not created by the main malicious executable.

**SisInfo.cfg is not included in the SISX package**

```
C:\sys\bin\Installer_0x20026CAA.exe
C:\sys\bin\MainSrv2.exe
C:\private\101f875a\import\[20026CA9].rsc
```

Strange: the Installer executable parses the SISX package file. Let's investigate...



```
 hexdump -C SisInfo.cfg
2f 2f 77  |........http://w|
63 6f 6d  |ww.megac1jck.com|
77 2e 6d  |....http://www.m|
00 00 68  |akt000b.com....h|
69 61 66  |ttp://www.mediaf|
74 70 3a  |ir8.com....http:|
30 61 64  |//www.megaup10ad|
2f 2f 77  |.com....http://w|
6d        |ww.mozi11a.com|
```

Figure: Where do those domain names come from ?

# Domain Name Decryption Assembly Code

Calling decryption func

```
SUB R0, R11, #0xBC
MOV R1, #0xBF
BL Yxes_decryptName
```

The key is **0xBF** !

# Domain Name Decryption Assembly Code

### Calling decryption func

```
SUB R0, R11, #0xBC
MOV R1, #0xBF
BL Yxes_decryptName
```

The key is **0xBF** !

### Yxes_decryptName gets arguments

```
MOV R12, SP
STMFD SP!, {R4, R11, R12, ...}
SUB R11, R12, #4
STR R0, [R11, #buffer]
MOV R3, R1
STRB R3, [R11, #key]
```

**arg 1**: buffer to decrypt, **arg 2**: key

# Domain Name Decryption Assembly Code

### Calling decryption func

```
SUB R0, R11, #0xBC
MOV R1, #0xBF
BL Yxes_decryptName
```

The key is **0xBF** !

### Yxes_decryptName gets arguments

```
MOV R12, SP
STMFD SP!, {R4, R11, R12, ...}
SUB R11, R12, #4
STR R0, [R11, #buffer]
MOV R3, R1
STRB R3, [R11, #key]
```

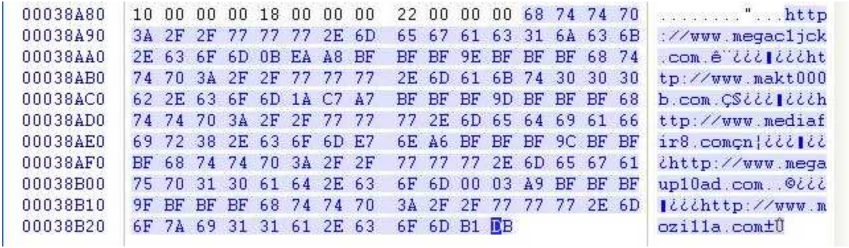
**arg 1**: buffer to decrypt, **arg 2**: key

### XOR decryption of character

```
LDR R0, [R11,#buffer]
LDR R1, [R11,#position]
BL Yxes_atC
MOV R4, R0
LDR R0, [R11, #buffer]
LDR R1, [R11, #position]
BL Yxes_atC
LDRB R2, [R0]
LDRB R3, [R11, #key]
EOR R3, R2, R3
STRB R3, [R4]
LDR R3, [R11, #position]
ADD R3, R3, #1
B Yxes_haveWeFinished
```

# Domain Names: solved!

Manually apply XOR with 0xBF to the end of the package (WebLocks.sisx, LanPackage.sisx ...)



```
00038A80   10 00 00 00 18 00 00 00  22 00 00 00 68 74 74 70   ........"...http
00038A90   3A 2F 2F 77 77 77 2E 6D  65 67 61 63 31 6A 63 6B   ://www.megac1jck
00038AA0   2E 63 6F 6D 0B EA A8 BF  BF BF 9E BF BF BF 68 74   .com.ê¨¿¿¿▮¿¿¿ht
00038AB0   74 70 3A 2F 2F 77 77 77  2E 6D 61 6B 74 30 30 30   tp://www.makt000
00038AC0   62 2E 63 6F 6D 1A C7 A7  BF BF BF 9D BF BF BF 68   b.com.Ç§¿¿¿▮¿¿¿h
00038AD0   74 74 70 3A 2F 2F 77 77  77 2E 6D 65 64 69 61 66   ttp://www.mediaf
00038AE0   69 72 38 2E 63 6F 6D E7  6E A6 BF BF BF 9C BF BF   ir8.comçn¦¿¿¿▮¿¿
00038AF0   BF 68 74 74 70 3A 2F 2F  77 77 77 2E 6D 65 67 61   ¿http://www.mega
00038B00   75 70 31 30 61 64 2E 63  6F 6D 00 03 A9 BF BF BF   up10ad.com..©¿¿¿
00038B10   9F BF BF BF 68 74 74 70  3A 2F 2F 77 77 77 2E 6D   ▮¿¿¿http://www.m
00038B20   6F 7A 69 31 31 61 2E 63  6F 6D B1 DB               ozi11a.com±Û
```

Figure: Decrypted domain names

Presenting SymbOS/Yxes

Global Overview

Finding URLs of Remote Servers

**Communication with Remote Servers**

Silent Installation

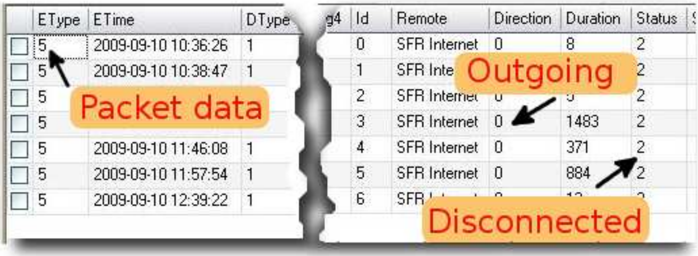
Proof or Guess?

# Silent Connection to Internet

- Yxes automatically selects an IAP (see cdbv3.dat)
- Stealth connections: disables the end-user dialog, only requires NetworkServices: "basic" capability !

```
TCommDbConnPref pref;
pref.SetDialogPreference(ECommDbDialogPrefDoNotPrompt);
```

- But communications logged in c:\101f401d\logdbu.dat



|  | EType | ETime | DType |
|---|---|---|---|
| □ | 5 | 2009-09-10 10:36:26 | 1 |
| □ | 5 | 2009-09-10 10:38:47 | 1 |
| □ | 5 | [illegible] | [illegible] |
| □ | 5 | [illegible] | [illegible] |
| □ | 5 | 2009-09-10 11:46:08 | 1 |
| □ | 5 | 2009-09-10 11:57:54 | 1 |
| □ | 5 | 2009-09-10 12:39:22 | 1 |

| Id | Remote | Direction | Duration | Status |
|---|---|---|---|---|
| 0 | SFR Internet | 0 | 8 | 2 |
| 1 | SFR Inte | [illegible] | [illegible] | 2 |
| 2 | SFR Internet | 0 | 5 | 2 |
| 3 | SFR Internet | 0 | 1483 | 2 |
| 4 | SFR Internet | 0 | 371 | 2 |
| 5 | SFR Internet | 0 | 884 | 2 |
| 6 | SFR | [illegible] | [illegible] | [illegible] |

# Communicating with Malicious Servers

Java Server Pages on the malicious servers:

- Retrieved from ill-configured malicious servers, different versions
- Returns ”pnpause” when unavailable
- Maintains blacklist of IPs :(

```
String ip = request.getRemoteAddr();
if(ip!=null && Definition.IP_BLACK_LIST.indexOf(ip+",")!=-1)
response.sendError(404);
return;
}
```

### Kernel.jsp

Download appropriate package depending on phone type

### PbkInfo.jsp

Upload victim's contact info on the server

### Number.jsp

Logs phone numbers, IMSI, IMEI

# Controlling Propagation

Localized files returned by the remote malicious servers:

- Tip.jsp: returns a localized file. SMS message ?

  ```
  fileName = service.getTipFile(sFileType, sLanguage);
  ```

- NumberFile.jsp returns a MCC-dependant file. Phone numbers within the country ?

  ```
  String fileName = service.getNumberFile(mcc);
  ```

- Information returned is encrypted or encoded ?

Indirect propagation via SMS:

- SMS: no attachment, includes a link
- MMS: limited support. 40% in France [source: Ocito]

- Presenting SymbOS/Yxes
- Global Overview
- Finding URLs of Remote Servers
- Communication with Remote Servers
- **Silent Installation**
- Proof or Guess?

# SW Installer Launcher API

Silent installation using the SW Installer Launcher API:

- Symbian API for S60 3rd edition phones
- A new class: RSWInstSilentLauncher

Installation steps:

1. Connect to the phone's internal install server

```
SwiUI::RSWInstSilentLauncher iLauncher;
iLauncher.Connect();
```

2. Install the SISX package

```
iLauncher.SilentInstall(reqStat, filename, options);
```

3. Close install server session

```
iLauncher.Close();
```

# Silent Installation of Malware

## Download Malware

Download Yxes variant from remote server

Store in C:\Data\kel.sisx (or root.sisx ...)

## Install Malware

```
LDR     R0, [R11,#installobj]
MOV     R1, R3          ; request status
LDR     R2, [R11,#filename]
MOV     R3, R12         ; options
BL      SWInstCli_4     ; RSWInstSilentLauncher::SilentInstall
```

## Cleanup

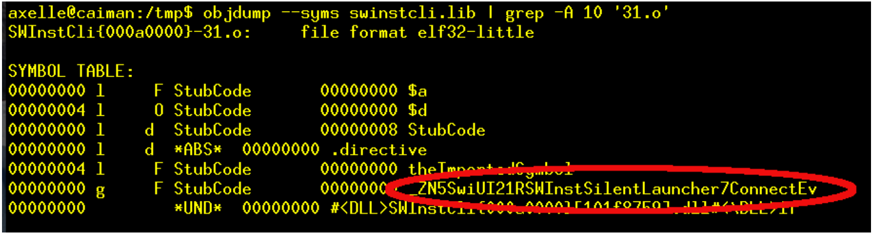
Close install server connection

Delete temporary file (e.g kel.sisx)

# Resolving API Names in Code

**Problem**: Names not automatically resolved...

```
BL SWInstCli_32
BL SWInstCli_31
BL SWInstCli_13
BL SWInstCli_4
```



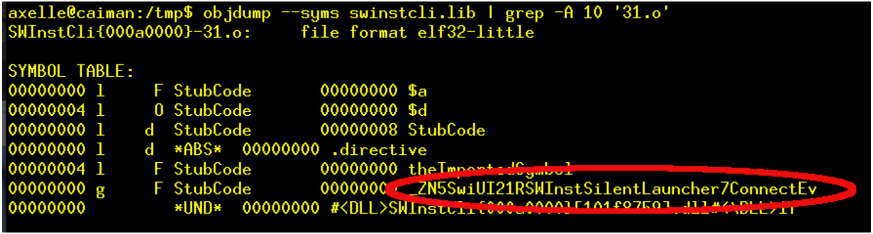
```
axelle@caiman:/tmp$ objdump --syms swinstcli.lib | grep -A 10 '31.o'
SWInstCli{000a0000}-31.o:     file format elf32-little

SYMBOL TABLE:
00000000 l     F StubCode       00000000 $a
00000004 l     O StubCode       00000000 $d
00000000 l    d  StubCode       00000008 StubCode
00000000 l    d  *ABS*  00000000 .directive
00000004 l     F StubCode       00000000 theImportedSymbol
00000000 g     F StubCode       00000000 _ZN5SwiUI21RSWInstSilentLauncher7ConnectEv
00000000         *UND*  00000000 #<DLL>SWInstCli{000a0000}[101f8759].dll#<\DLL>1f
```

# Resolving API Names in Code

**Problem**: Names not automatically resolved...

| | |
|---|---|
| `BL SWInstCli_32` | RSWInstSilentLauncher constructor |
| `BL SWInstCli_31` | Connect |
| `BL SWInstCli_13` | Close |
| `BL SWInstCli_4` | SilentInstall |



```
axelle@caiman:/tmp$ objdump --syms swinstcli.lib | grep -A 10 '31.o'
SWInstCli{000a0000}-31.o:     file format elf32-little

SYMBOL TABLE:
00000000 l     F StubCode       00000000 $a
00000004 l     O StubCode       00000000 $d
00000000 l    d  StubCode       00000008 StubCode
00000000 l    d  *ABS*  00000000 .directive
00000004 l     F StubCode       00000000 theImportedSymbol
00000000 g     F StubCode       00000000 _ZN5SwiUI21RSWInstSilentLauncher7ConnectEv
00000000         *UND*  00000000 #<DLL>SWInstCli{000a0000}[101f8759].dll#<\DLL>1f
```

Presenting SymbOS/Yxes

Global Overview

Finding URLs of Remote Servers

Communication with Remote Servers

Silent Installation

Proof or Guess?

# Quick assumptions (no offense meant!)

### Propagates to all contacts - Partially WRONG

**Proof**: sends SMS to *unknown* phone numbers

### Botnet or not?

Communication with remote servers: YES

Commands and controls: not really

### "Only present on Nokia 3250 handsets" - WRONG

Nokia 3250 is the default phone type string !

Affects S60 3rd edition phones

### Yxes replicates on the phone as root.sisx... - WRONG

This is the name of the file in which the remote malware is dumped

Root.sisx contains *another variant* of Yxes.

# SymbOS/Yxes worm: status

| Functionality | Proof exists or guess? |
|---|---|
| Contacts remote web servers | PROOF |
| **Remote server URLs encrypted at the end of SISX package** | PROOF |
| Sends SMS message | PROOF |
| SMS Text is sent by TipFile.jsp | SENSIBLE GUESS |
| SMS recipient phone number sent by NumberFile.jsp | SENSIBLE GUESS |
| Sends phone numbers of contacts | PROOF |
| Reads/sends phone's IMEI, IMSI... | PROOF |
| **Installs other variants of itself** | PROOF |
| Automatically restarts when phone is rebooted | PROOF |
| Only one instance of the malware may run at a time | PROOF |
| Uses cryptography | GUESS |
| Currently in debug status | GUESS |

# To do next...

Missing pieces in the puzzle:

- Where does the SMS text come from?
- Decrypt data sent by the servers
- The malware checks for a string "olpx": what does it mean?
- Cyber-crime angle unclear: debugging status currently

Only few tools for phone analysis:

- Step by step debugging with IDA Pro
- Forensic tools to read phone logs
- No packet sniffer, disable network...

# Questions?

Hope you enjoyed it!

Any questions?

mailto: axelle@fortinet.com

Slides edited with BeamerEditor

# Counter mobile malware [BACKUP]

## Non technical solutions

- Educate end-users to "smell" malicious applications Won't solve all issues
- Sue malware authors (legal combat) Difficult to do
- Display SMS and call costs explicitly Operators?

## Technical solutions

- Install an anti-virus ;) Unknown viruses...
- SMS sending and contact parsing requires extended capability Would not stop Yxes
- Filter SMS messages delicate
- Sensitive data or operations locked by password? burden
- ...

# Yxes variants specificities [BACKUP]

- A: first variant (Feb 2009).
- B: does not install. Signed with a developer certificate (basic capabilities only)
- C: mentions a PRGKEY and Rijndael. Parses contacts.
- D: sexy.sisx executes CallMasterD.exe (personal interactive voice response). SKServer_hide.sisx contains SMS text 'A very interesting sexy game!'... Sends only its own phone number to servers, not all contacts.
- E: WebGate_Locks.sisx trojans 'Advanced Device Locks' application. Encrypted URLs at the enf of the SISX file.
- F: sends vCards of all contacts to remote server. Does not send SMS.
- G: randomly picks up a number from remote server list, and sends an SMS to that number (sensible guess)
- H: latest variant (March 2010). Uses remote, local and kernel parameters. Uses different remote servers than E.

# Sending an SMS [BACKUP]

### Initiate SMS Send As server

```
RSendAs sendas;
sendas.Connect();
RSendAsmessage msg;
msg.CreateL(&sendas, KSenduiMtmSmsUid);
```

### Add recipient and text

```
msg.AddRecipientL( phonenumber,
         RSendAsMessage::ESendAsRecipientTo);
msg.SetBodyTextL( the text )
```

### Send!

```
msg.SendMessageAndCloseL();
```