When E.T. comes into Windows Mobile 6

a.k.a. PoC(k)ET

Cedric Halbronn
Sogeti / ESEC R&D
`cedric(at)security-labs.org`

Hack.lu 2009

1. Context / Objectives
2. Technical aspects of WM6
3. Implementation
   - General architecture
   - Injection
   - Protection
   - Backdoor
   - Services
4. Demo

Context

Who am I?

- Security researcher working at Sogeti ESEC R&D lab
- Focusing on mobile security

A smartphone?

- Mobile phone → smartphone
- Various services
  - PDA, Web, camera, GPS, microphone, etc.
- Current OS :
  - Symbian, RIM OS, Windows Mobile 6, iPhone OS, Android
- Studies on mobile phones rootkits capabilities still limited

Context

Who am I?

- Security researcher working at Sogeti ESEC R&D lab
- Focusing on mobile security

A smartphone?

- Mobile phone → smartphone
- Various services
  - PDA, Web, camera, GPS, microphone, etc.
- Current OS :
  - Symbian, RIM OS, Windows Mobile 6, iPhone OS, Android
- Studies on mobile phones rootkits capabilities still limited

Objectives

TODO list

Develop a rootkit for WM6

What is a “rootkit”?

- Post-exploitation
- Components:
  - Injection
  - Protection
  - Backdoor
  - Services

Taking into account...

- Embedded constraints / mobile environment
- Services on the table

Objectives

TODO list

Develop a rootkit for WM6

What is a "rootkit"?

- Post-exploitation
- Components:
  - Injection
  - Protection
  - Backdoor
  - Services

Taking into account...

- Embedded constraints / mobile environment
- Services on the table

Objectives

TODO list

Develop a rootkit for WM6

What is a "rootkit"?

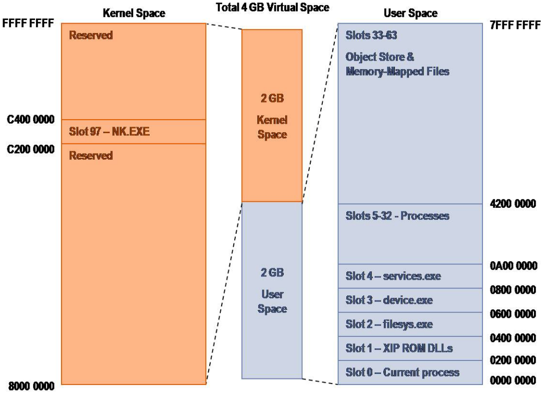
- Post-exploitation
- Components:
  - Injection
  - Protection
  - Backdoor
  - Services

Taking into account...

- Embedded constraints / mobile environment
- Services on the table

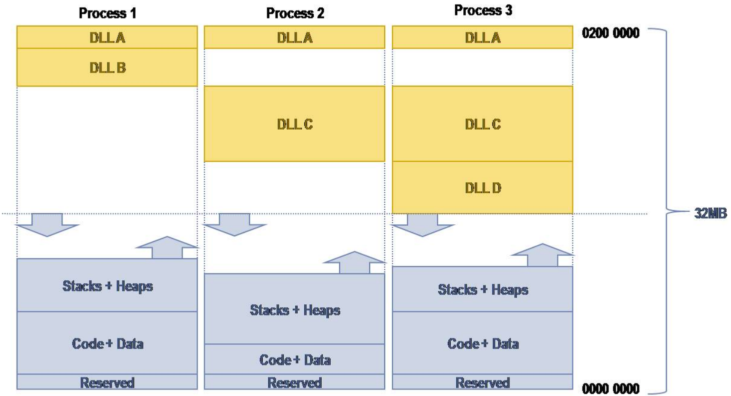
1. Context / Objectives
2. Technical aspects of WM6
3. Implementation
   - General architecture
   - Injection
   - Protection
   - Backdoor
   - Services
4. Demo

Virtual Memory Address Space



Global Virtual Memory Address Space (4GB)

Loading DLLs



Loading DLLs under Windows Mobile 6

Security policies

Where?

Registry: [HKLM\Security\Policies\Policies]

Some examples

Policy	ID	Description
Auto Run Policy	"2"	0 (allowed to run automatically), 1 (restricted)
Unsigned Applications Policy	"1006"	1 (allowed to run), 0 (not allowed to run)
Unsigned Prompt Policy	"101A"	0 (user will be prompted), 1 (user will not be prompted)
Password Required Policy	"1023"	0 (a password is required), any other (a password is not required)

Security policies

Where?

Registry: [HKLM\Security\Policies\Policies]

Some examples

Policy	ID	Description
Auto Run Policy	"2"	0 (allowed to run automatically), 1 (restricted)
Unsigned Applications Policy	"1006"	1 (allowed to run), 0 (not allowed to run)
Unsigned Prompt Policy	"101A"	0 (user will be prompted), 1 (user will not be prompted)
Password Required Policy	"1023"	0 (a password is required), any other (a password is not required)

Application signing

Stores for code execution

- Privileged store: privileged execution trust authorities
- Unprivileged store: unprivileged execution trust authorities
- SPC (Software Publisher Certificates) store: trust authorities for CAB installation
  → sign DLLs, EXEs or CABs and put certificate in right store

Stores for SSL chain validation, NOTHING to do with code execution

- MY: end-user personal certificates
- CA: intermediary certification authorities certificates
- ROOT: root (self-signed) certificates

Application signing

Stores for code execution

- Privileged store: privileged execution trust authorities
- Unprivileged store: unprivileged execution trust authorities
- SPC (Software Publisher Certificates) store: trust authorities for CAB installation
  → sign DLLs, EXEs or CABs and put certificate in right store

Stores for SSL chain validation, NOTHING to do with code execution

- MY: end-user personal certificates
- CA: intermediary certification authorities certificates
- ROOT: root (self-signed) certificates

1. Context / Objectives
2. Technical aspects of WM6
3. Implementation
   - General architecture
   - Injection
   - Protection
   - Backdoor
   - Services
4. Demo

Plan

1. Context / Objectives
2. Technical aspects of WM6
3. Implementation
   - General architecture
   - Injection
   - Protection
   - Backdoor
   - Services
4. Demo

Technical choices

Architecture

- Hide its presence from phone's user
- Expatriate information

Technical choices

- 32-process limit → Single .EXE multi-threads
- DLLs impact → limit their size
- Battery usage → limit actions when needed
- Heterogeneous environment

Technical choices

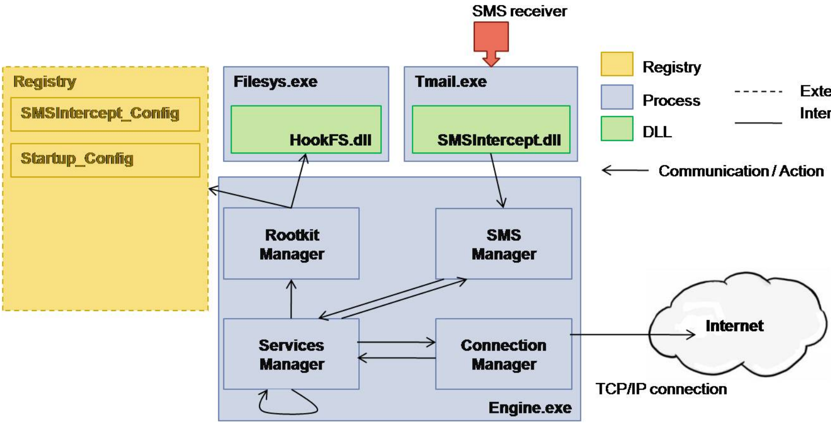
Architecture

- Hide its presence from phone's user
- Expatriate information

Technical choices

- 32-process limit → Single .EXE multi-threads
- DLLs impact → limit their size
- Battery usage → limit actions when needed
- Heterogeneous environment

Architecture



Rootkit general architecture

Plan

1. Context / Objectives
2. Technical aspects of WM6
3. Implementation
   - General architecture
   - Injection
   - Protection
   - Backdoor
   - Services
4. Demo

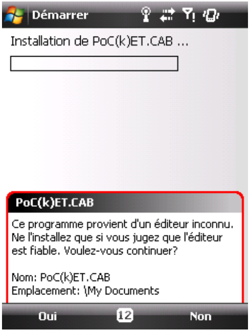
Rootkit injection

Injection methods

- Smartphone access
- Vulnerability exploit
  → Ex: MMS handler in WM2003
- WAP Push message
  - Web link
    → Ex: Etisalat operator in the United Arab Emirates (UAE) for Blackberries
  - OTA provisioning

Our context

- Smartphone access
- Unsigned CAB → Pop-up



Installation de PoC(k)ET.CAB ...

PoC(k)ET.CAB

Ce programme provient d'un éditeur inconnu. Ne l'installez que si vous jugez que l'éditeur est fiable. Voulez-vous continuer?

Nom: PoC(k)ET.CAB
Emplacement: \My Documents

Pop-up

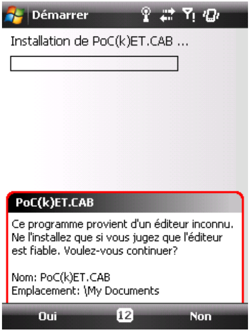
Rootkit injection

Injection methods

- Smartphone access
- Vulnerability exploit
  → Ex: MMS handler in WM2003
- WAP Push message
  - Web link
    → Ex: Etisalat operator in the United Arab Emirates (UAE) for Blackberries
  - OTA provisioning

Our context

- Smartphone access
- Unsigned CAB → Pop-up



Installation de PoC(k)ET.CAB ...

PoC(k)ET.CAB

Ce programme provient d'un éditeur inconnu. Ne l'installez que si vous jugez que l'éditeur est fiable. Voulez-vous continuer?

Nom: PoC(k)ET.CAB
Emplacement: \My Documents

Pop-up

Plan

1. Context / Objectives
2. Technical aspects of WM6
3. Implementation
   - General architecture
   - Injection
   - Protection
   - Backdoor
   - Services
4. Demo

Automatic startup for an application

Auto-start methods

- *[HKLM\Init]*
- *\Windows\Startup*
- Create a service
  → DLL loaded by *Services.exe*

Our choice

\Windows\Startup

Automatic startup for an application

Auto-start methods

- *[HKLM\Init]*
- *\Windows\Startup*
- Create a service
  → DLL loaded by *Services.exe*

Our choice

\Windows\Startup

Hide unsigned apps (1/2)

By default

Necessary so we do NOT alert the phone user

First attempt

Disable the unsigned prompt policy

[HKLM\Security\Policies\Policies] ”0000101a”=dword:1

Result

Not good, because all external unsigned applications will run without alerting the user

Hide unsigned apps (1/2)

By default

Necessary so we do NOT alert the phone user

First attempt

Disable the unsigned prompt policy
[HKLM\Security\Policies\Policies] ”0000101a”=dword:1

Result

Not good, because all external unsigned applications will run without alerting the user

Hide unsigned apps (1/2)

By default

Necessary so we do NOT alert the phone user

First attempt

Disable the unsigned prompt policy

[HKLM\Security\Policies\Policies] "0000101a"=dword:1

Result

Not good, because all external unsigned applications will run without alerting the user

Hide unsigned apps (2/2)

Second attempt

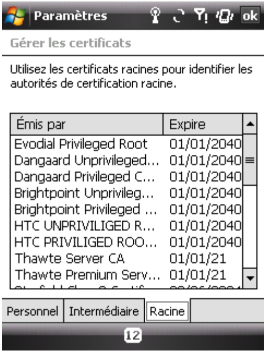
- Better to have our own certificate
- We can sign our binaries and put our certificate in Privileged store

Visible stores on the device

- MY, CA, ROOT
- Other stores are NOT visible

Result

Our own certificate will not be visible on the device



Gérer les certificats

Utilisez les certificats racines pour identifier les autorités de certification racine.

Émis par	Expire
Evodial Privileged Root	01/01/2040
Dangaard Unprivileged...	01/01/2040
Dangaard Privileged C...	01/01/2040
Brightpoint Unprivileg...	01/01/2040
Brightpoint Privileged ...	01/01/2040
HTC UNPRIVILIGED R...	01/01/2040
HTC PRIVILIGED ROO...	01/01/2040
Thawte Server CA	01/01/21
Thawte Premium Serv...	01/01/21

Visible certificate stores

Hide unsigned apps (2/2)

Second attempt

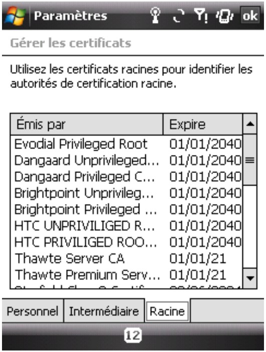
- Better to have our own certificate
- We can sign our binaries and put our certificate in Privileged store

Visible stores on the device

- MY, CA, ROOT
- Other stores are NOT visible

Result

Our own certificate will not be visible on the device



Gérer les certificats

Utilisez les certificats racines pour identifier les autorités de certification racine.

Émis par	Expire
Evodial Privileged Root	01/01/2040
Dangaard Unprivileged...	01/01/2040
Dangaard Privileged C...	01/01/2040
Brightpoint Unprivileg...	01/01/2040
Brightpoint Privileged ...	01/01/2040
HTC UNPRIVILIGED R...	01/01/2040
HTC PRIVILIGED ROO...	01/01/2040
Thawte Server CA	01/01/21
Thawte Premium Serv...	01/01/21

Visible certificate stores

Hide unsigned apps (2/2)

Second attempt

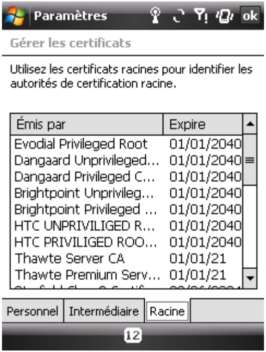
- Better to have our own certificate
- We can sign our binaries and put our certificate in Privileged store

Visible stores on the device

- MY, CA, ROOT
- Other stores are NOT visible

Result

Our own certificate will not be visible on the device



Gérer les certificats

Utilisez les certificats racines pour identifier les autorités de certification racine.

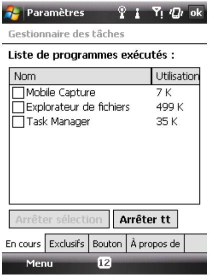
Émis par	Expire
Evodial Privileged Root	01/01/2040
Dangaard Unprivileged...	01/01/2040
Dangaard Privileged C...	01/01/2040
Brightpoint Unprivileg...	01/01/2040
Brightpoint Privileged ...	01/01/2040
HTC UNPRIVILIGED R...	01/01/2040
HTC PRIVILIGED ROO...	01/01/2040
Thawte Server CA	01/01/21
Thawte Premium Serv...	01/01/21

Visible certificate stores

Hide processes (1/2)

First attempt

- By default, not needed. Task Manager does NOT show them
- Apparently, it does not show processes that do not have a visible window.

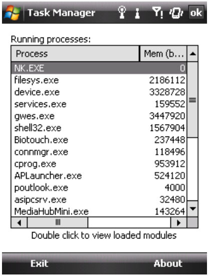


Gestionnaire des tâches

Liste de programmes exécutés :

Nom	Utilisation
□ Mobile Capture	7 K
□ Explorateur de fichiers	499 K
□ Task Manager	35 K

WM6 TaskManager



Running processes:

Process	Mem (b...
NK.EXE	0
filesys.exe	2186112
device.exe	3328728
services.exe	159552
gwes.exe	3447920
shell32.exe	1567904
Biotouch.exe	237448
connmgr.exe	118496
cprog.exe	953912
APLauncher.exe	524120
poutlook.exe	4000
asipcsrv.exe	32480
MediaHubMini.exe	143264

Double click to view loaded modules

TaskManagerCE by K. Varma (c)

Hide processes (2/2)

Second attempt

- For better results, possible to hide them a little bit more.
- Using method from Petr Matousek (2007).

Details

- No doubly-linked list here
- 32 processes are stored in a `PPROCESS table[32];`
- Function listing the processes
  - Browses this table
  - Verifies a condition on the process name to consider the slot used
  - Putting the name to `NULL` → it is NOT listed

Hide processes (2/2)

Second attempt

- For better results, possible to hide them a little bit more.
- Using method from Petr Matousek (2007).

Details

- No doubly-linked list here
- 32 processes are stored in a `PPROCESS table[32];`
- Function listing the processes
  - Browses this table
  - Verifies a condition on the process name to consider the slot used
  - Putting the name to `NULL` → it is NOT listed

Hide files

First attempt

At first, not needed, who browse files on mobile phones?

Second attempt

- For better results, possible to hide them a little bit more.
- Using method from Petr Matousek (2007).

Details

- Inject a DLL into the process handling the file system functions
- Hook the file listing functions: `FindFirstFileW`, `FindNextFileW`

Hide files

First attempt

At first, not needed, who browse files on mobile phones?

Second attempt

- For better results, possible to hide them a little bit more.
- Using method from Petr Matousek (2007).

Details

- Inject a DLL into the process handling the file system functions
- Hook the file listing functions: `FindFirstFileW`, `FindNextFileW`

Hide files

First attempt

At first, not needed, who browse files on mobile phones?

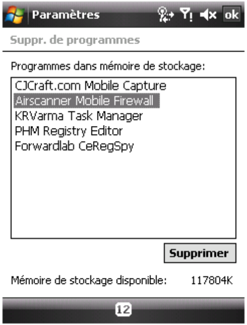
Second attempt

- For better results, possible to hide them a little bit more.
- Using method from Petr Matousek (2007).

Details

- Inject a DLL into the process handling the file system functions
- Hook the file listing functions: `FindFirstFileW`, `FindNextFileW`

Hide CAB installation (1/3)



Programmes dans mémoire de stockage:

- CJCraft.com Mobile Capture
- Airscanner Mobile Firewall
- KRVarma Task Manager
- PHM Registry Editor
- Forwardlab CeRegSpy

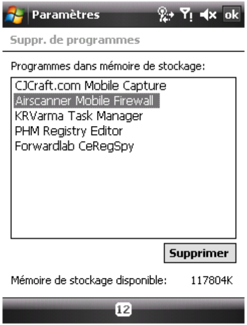
Mémoire de stockage disponible: 117804K

Add/Remove Programs

CAB installation management

- *[HKLM\Security\AppInstall]*
- A key is created in it for the installed app

Hide CAB installation (1/3)



Programmes dans mémoire de stockage:

CJCraft.com Mobile Capture
Airscanner Mobile Firewall
KRVarma Task Manager
PHM Registry Editor
Forwardlab CeRegSpy

Mémoire de stockage disponible: 117804K

Add/Remove Programs

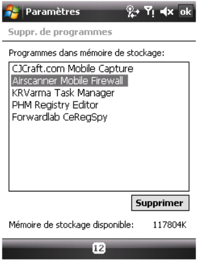
CAB installation management

- *[HKLM\Security\AppInstall]*
- A key is created in it for the installed app

Hide CAB installation (2/3)

First attempt

- Method taken from Airscanner Mobile Firewall
- When putting the value “Role” to 0, it disappear from the list

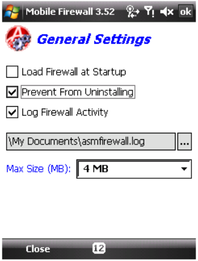


Suppr. de programmes

Programmes dans mémoire de stockage:

CJCraft.com Mobile Capture
Airscanner Mobile Firewall
KRVarma Task Manager
PHM Registry Editor
Forwardlab CeRegSpy

Mémoire de stockage disponible: 117804K



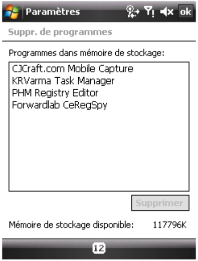
General Settings

☐ Load Firewall at Startup
☑ Prevent From Uninstalling
☑ Log Firewall Activity

\My Documents\asmfirewall.log

Max Size (MB): 4 MB

Airscanner Mobile Firewall (c)



Suppr. de programmes

Programmes dans mémoire de stockage:

CJCraft.com Mobile Capture
KRVarma Task Manager
PHM Registry Editor
Forwardlab CeRegSpy

Mémoire de stockage disponible: 117796K

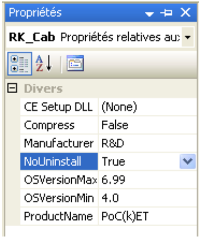
Hide CAB installation (3/3)

Second attempt

In visual studio, specify the *"NoUninstall"* option in CAB project

Result

- Do not create a key in *[HKLM\Security\AppInstall]*
- No way to detect it in the registry



Propriétés

RK_Cab Propriétés relatives au:

⊟ Divers

CE Setup DLL	(None)
Compress	False
Manufacturer	R&D
NoUninstall	True
OSVersionMax	6.99
OSVersionMin	4.0
ProductName	PoC(k)ET

NoUninstall option

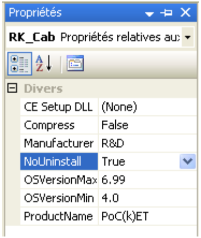
Hide CAB installation (3/3)

Second attempt

In visual studio, specify the *"NoUninstall"* option in CAB project

Result

- Do not create a key in *[HKLM\Security\AppInstall]*
- No way to detect it in the registry



Divers

CE Setup DLL	(None)
Compress	False
Manufacturer	R&D
NoUninstall	True
OSVersionMax	6.99
OSVersionMin	4.0
ProductName	PoC(k)ET

NoUninstall option

Plan

1. Context / Objectives
2. Technical aspects of WM6
3. Implementation
    - General architecture
    - Injection
    - Protection
    - Backdoor
    - Services
4. Demo

TCP/IP communication

Means of communication

- "Data" networks: GPRS, Edge, 3G
- Wi-Fi
- ActiveSync

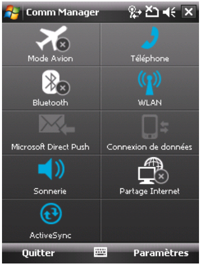
How to do it?

Phone is behind a NAT

→ A TCP/IP server on the attacker's side

Save battery life

Detect a connection → then, use it.



Communication Manager

TCP/IP communication

Means of communication

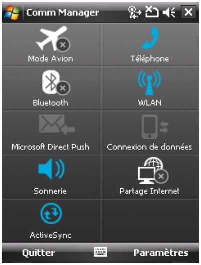
- “Data” networks: GPRS, Edge, 3G
- Wi-Fi
- ActiveSync

How to do it?

Phone is behind a NAT
→ A TCP/IP server on the attacker’s side

Save battery life

Detect a connection → then, use it.



Communication Manager

TCP/IP communication

Means of communication

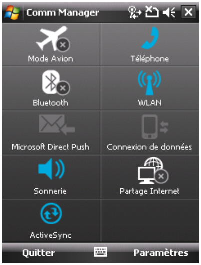
- "Data" networks: GPRS, Edge, 3G
- Wi-Fi
- ActiveSync

How to do it?

Phone is behind a NAT
→ A TCP/IP server on the attacker's side

Save battery life

Detect a connection → then, use it.



Communication Manager

An alternative means?

Problem

How to control the device when there is no "Data" connectivity?
→ Necessary to find an alternative means of communication

SMS messages

Command SMS → intercepted

Standard COM registration	HKEY_CLASSES_ROOT\CLSID\<clsid>\InProcServer32 @="SMSIntercept.dll"
MAPI Inbox	HKEY_LOCAL_MACHINE\Software\Microsoft\Inbox\Svc\SMS\Rules <clsid>=dword:1

<clsid> represents the COM object's class ID GUID.

Registry keys defined to intercept SMS messages

Side effect

When intercepting an SMS, the phone automatically switches on.

An alternative means?

Problem

How to control the device when there is no "Data" connectivity?
→ Necessary to find an alternative means of communication

SMS messages

Command SMS → intercepted

Standard COM registration	HKEY_CLASSES_ROOT\CLSID\<clsid>\InProcServer32 @="SMSIntercept.dll"
MAPI Inbox	HKEY_LOCAL_MACHINE\Software\Microsoft\Inbox\Svc\SMS\Rules <clsid>=dword:1

<clsid> represents the COM object's class ID GUID.

Registry keys defined to intercept SMS messages

Side effect

When intercepting an SMS, the phone automatically switches on.

An alternative means?

Problem

How to control the device when there is no "Data" connectivity?
→ Necessary to find an alternative means of communication

SMS messages

Command SMS → intercepted

Standard COM registration	HKEY_CLASSES_ROOT\CLSID\<clsid>\InProcServer32 @="SMSIntercept.dll"
MAPI Inbox	HKEY_LOCAL_MACHINE\Software\Microsoft\Inbox\Svc\SMS\Rules <clsid>=dword:1
<clsid> represents the COM object's class ID GUID.	

Registry keys defined to intercept SMS messages

Side effect

When intercepting an SMS, the phone automatically switches on.

An alternative means?

Problem

How to control the device when there is no “Data” connectivity?
→ Necessary to find an alternative means of communication

SMS messages

Command SMS → intercepted

Standard COM registration	HKEY_CLASSES_ROOT\CLSID\<clsid>\InProcServer32 @=”SMSIntercept.dll”
MAPI Inbox	HKEY_LOCAL_MACHINE\Software\Microsoft\Inbox\Svc\SMS\Rules <clsid>=dword:1

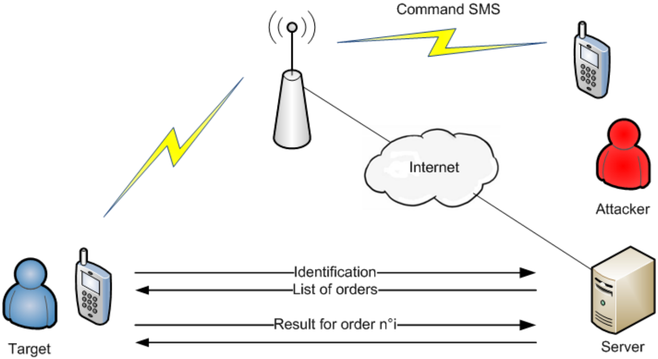
<clsid> represents the COM object’s class ID GUID.

Registry keys defined to intercept SMS messages

Side effect

When intercepting an SMS, the phone automatically switches on.

Protocol



Communication protocol

Plan

1. Context / Objectives
2. Technical aspects of WM6
3. Implementation
   - General architecture
   - Injection
   - Protection
   - Backdoor
   - Services
4. Demo

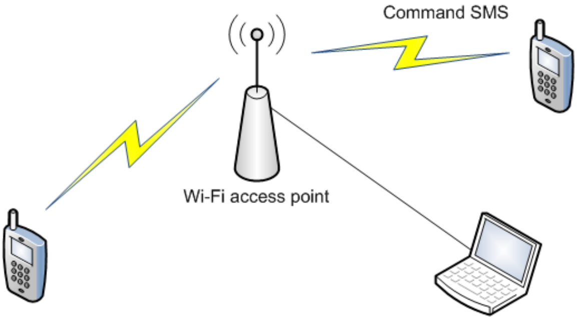
Services

Services on the table

- **Contacts**: last name, first name, mobile phone
- **SMS**: delivery time, sender, content
- **E-mails**: sender, recipients, delivery time, subject, content
- **GPS**: latitude, longitude
    - Registers to the OS
    - Notification when data are available

1. Context / Objectives
2. Technical aspects of WM6
3. Implementation
   - General architecture
   - Injection
   - Protection
   - Backdoor
   - Services
4. Demo

Demo



Conclusion

Results

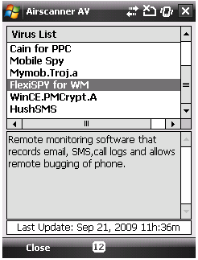
- Not detected by AVs
- Only detectable if we know where to look for

Limits / enhancement

- DLLs, registry keys, network connections
- Compression / encryption of communications
- Services : phone-tapping, microphone, camera. . .

Attacker point of view

- Win32 APIs but embedded constraints
- What about the other mobile OS?



Cain for PPC
Mobile Spy
Mymob.Troj.a
FlexiSPY for WM
WinCE.PMCrypt.A
HushSMS

Remote monitoring software that records email, SMS,call logs and allows remote bugging of phone.

Last Update: Sep 21, 2009 11h:36m

Airscanner Antivirus

Conclusion

Results

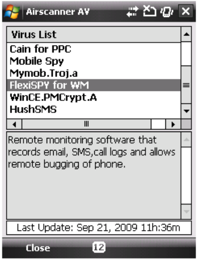
- Not detected by AVs
- Only detectable if we know where to look for

Limits / enhancement

- DLLs, registry keys, network connections
- Compression / encryption of communications
- Services : phone-tapping, microphone, camera. . .

Attacker point of view

- Win32 APIs but embedded constraints
- What about the other mobile OS?



Virus List
Cain for PPC
Mobile Spy
Mymob.Troj.a
FlexiSPY for WM
WinCE.PMCrypt.A
HushSMS

Remote monitoring software that records email, SMS,call logs and allows remote bugging of phone.

Last Update: Sep 21, 2009 11h:36m

Airscanner Antivirus

Conclusion

Results

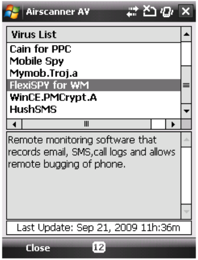
- Not detected by AVs
- Only detectable if we know where to look for

Limits / enhancement

- DLLs, registry keys, network connections
- Compression / encryption of communications
- Services : phone-tapping, microphone, camera. . .

Attacker point of view

- Win32 APIs but embedded constraints
- What about the other mobile OS?



Virus List

Cain for PPC
Mobile Spy
Mymob.Troj.a
FlexiSPY for WM
WinCE.PMCrypt.A
HushSMS

Remote monitoring software that records email, SMS,call logs and allows remote bugging of phone.

Last Update: Sep 21, 2009 11h:36m

Airscanner Antivirus

Questions?

Thank you for your attention