FORTINET

Defeating mTANs for profit

Axelle Apvrille, Kyle Yang

ShmooCon, January 2011

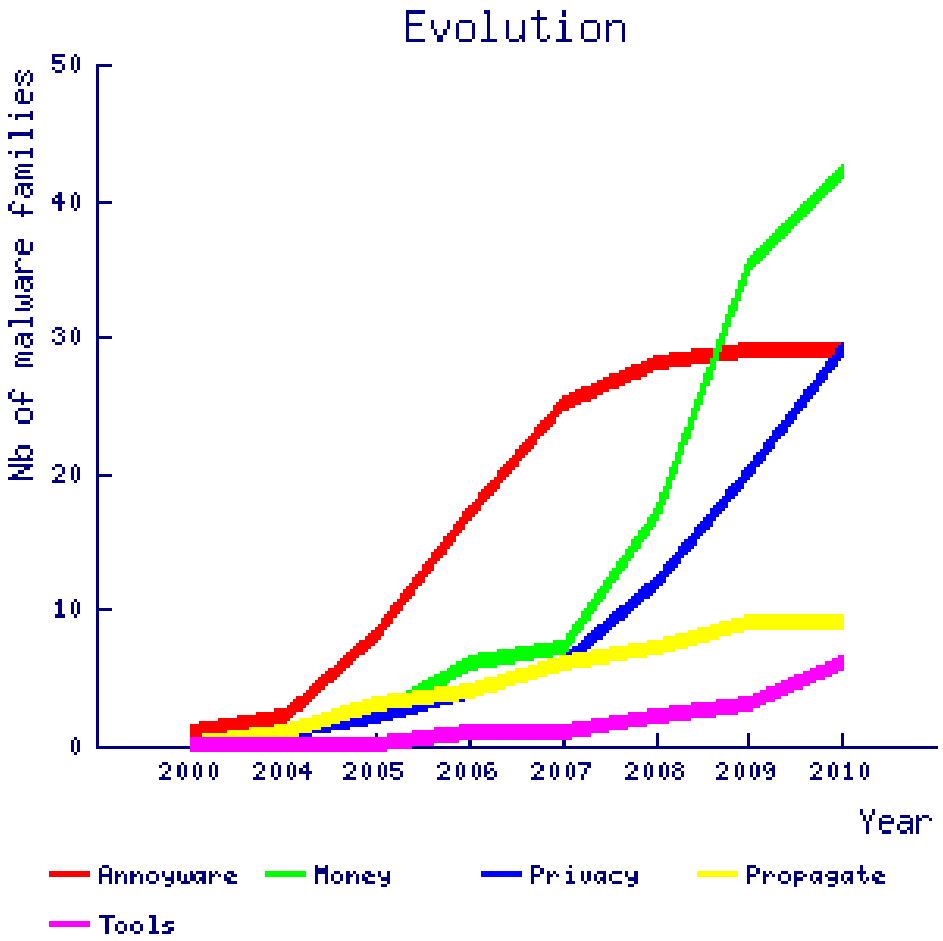
Summary

Zitmo? ... what the fuss?!

- first case of use by organized criminals

In brief

- **Z**eus **I**n **T**he **MO**bile
- Malware for Symbian phones (OS $>$ 9.0)
- Intercepts mTANs = one-time passwords sent by SMS
- Targetting Spanish online banks
- Propagated on PC by Zeus botnet



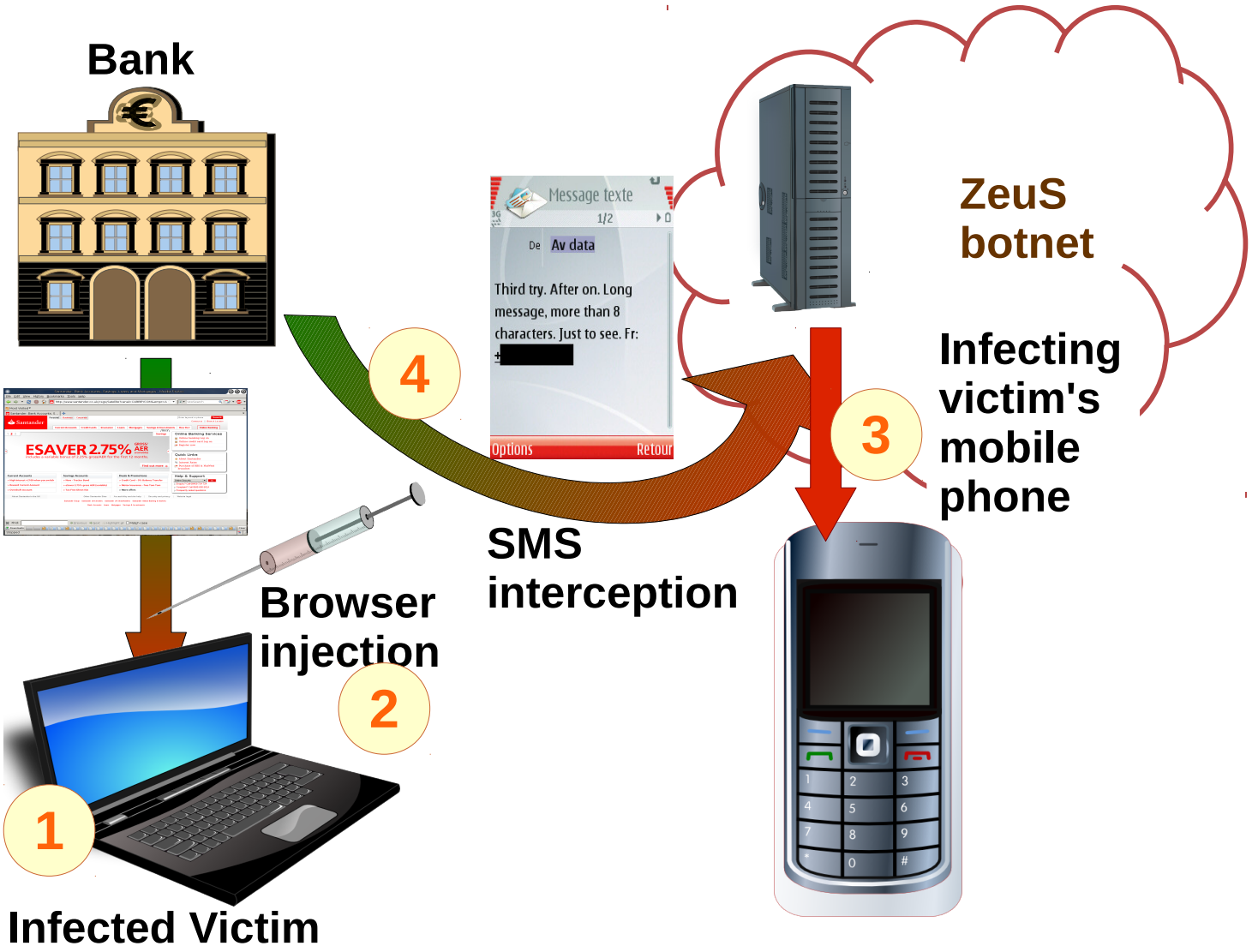
Zeus (aka Zbot): background

- It's a crimeware kit, sold in the underground market
- Designed to steal banking information
- There are *several* Zeus botnets, not only one

What's new for Zitmo's propagation?

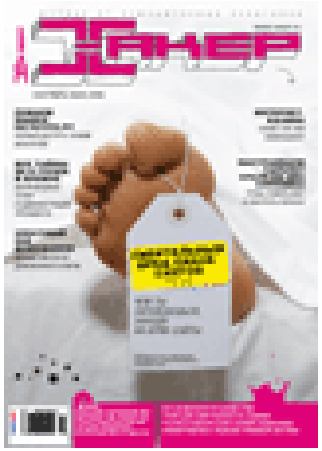
- Not 'much', because fully configurable
- Uses a different RC4 key to decrypt the configuration file
- Targets Spanish banks, injects Javascript into those URLs

Zitmo in a nutshell



Similarities with SMS Monitor

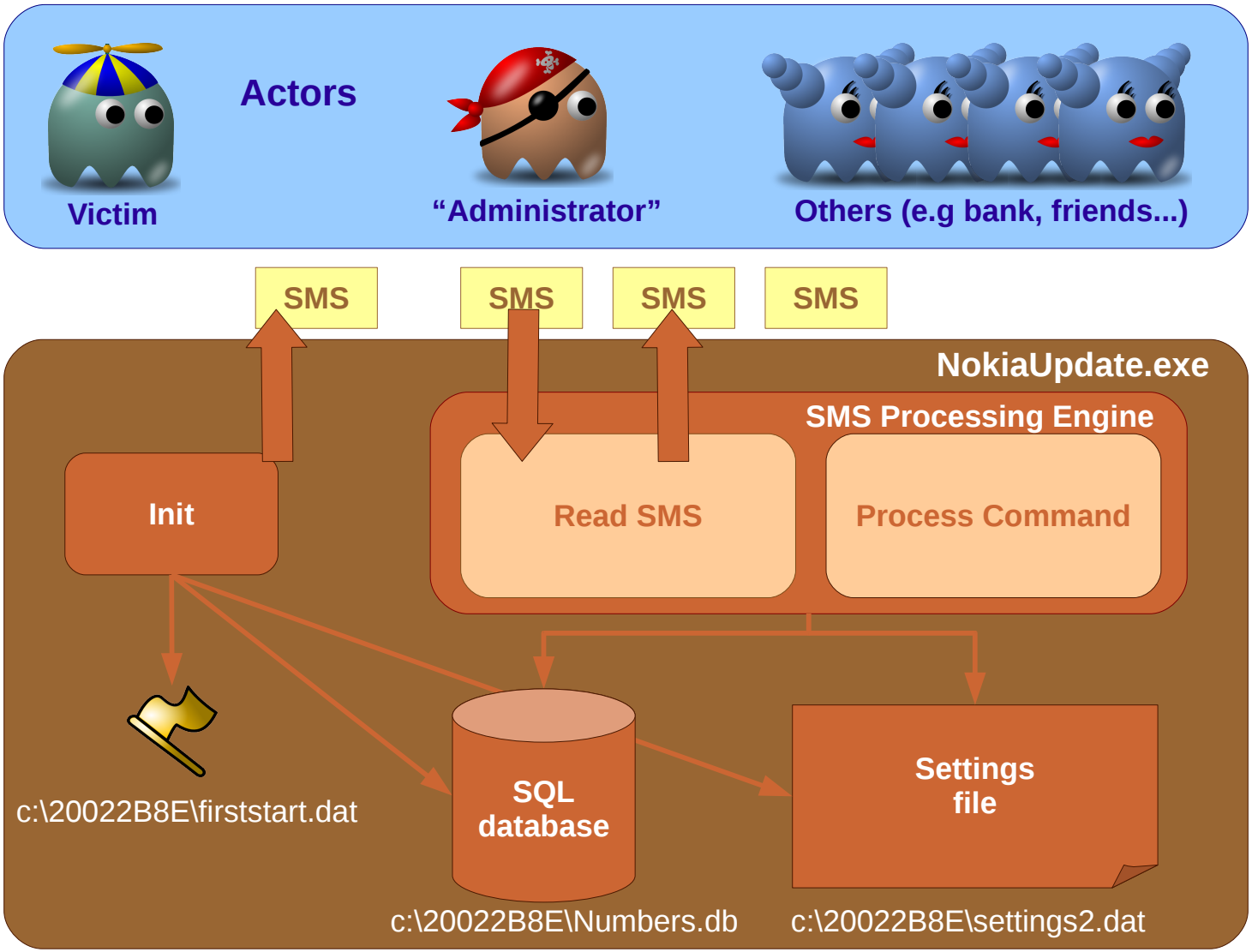
- SMS Monitor : "*The main purpose of this application is parental controls and security audit.*"
- Two papers in Russian Хакер magazine, with code: re-used by Zeus gang?



Zitmo compared with ...	Exact match of code same assembly	Exact match of strings case-sensitive match
SMS Monitor Lite	60%	89%
SMS Monitor	59%	90%
SymbOS/-Trapsms.A!tr.spy	13%	2%
SymbOS/-Fwdsms.D!tr.spy	16%	30%

Summary

[A Malware] Developer's Overview

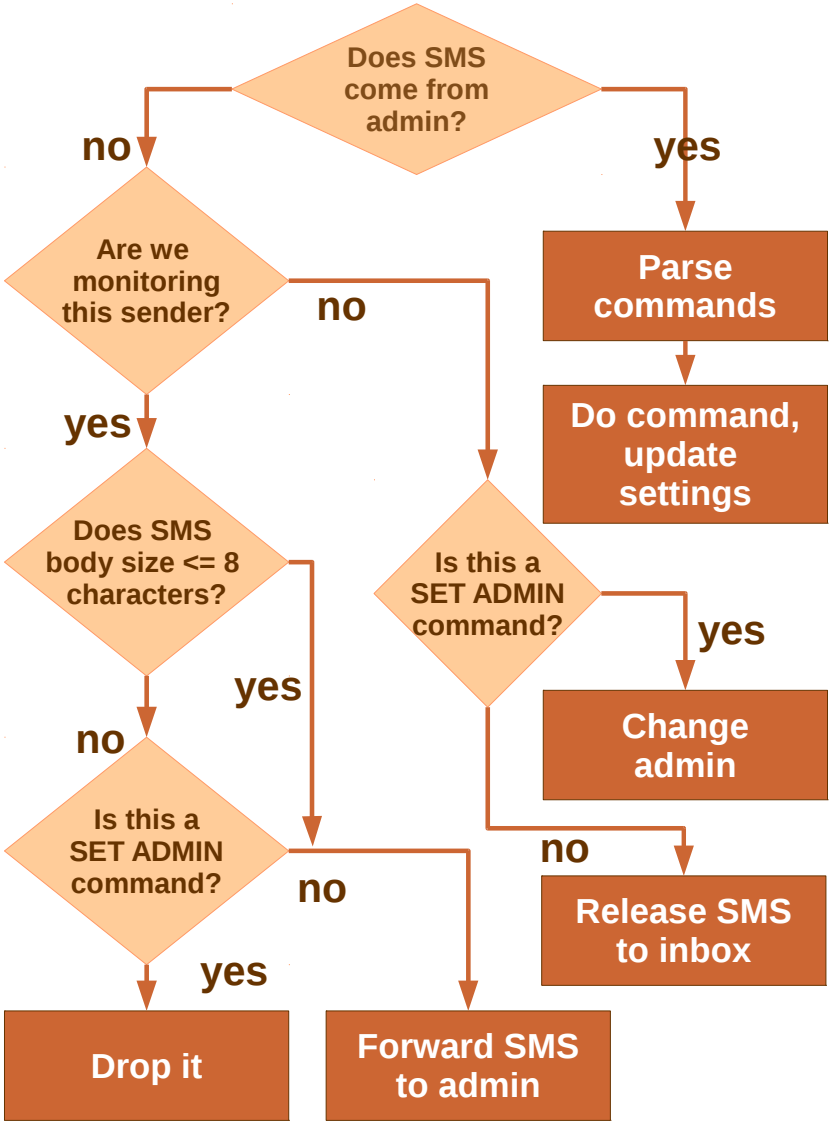


Silently intercept all SMS

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
; set socket family (SetSmsAddrFamily) to ESmsAddrMatchText
NL      _ZN8TSmsAddr16SetSmsAddrFamilyE14TSmsAddrFamily
SUB     R0, R11, #0x54
SUB     R3, R11, #0x24
MOV     R1, R3           ; text to match: _L8("")
BL      _ZN8TSmsAddr12SetTextMatchERK6TDesC8
```

Processing incoming SMS *(listen - new stuff here ;)*



Actions

- **Drop SMS**: nobody will ever see this SMS.
- **Forward SMS**: the SMS is sent to the administrator. Not displayed on the victim's phone.
- **Release SMS**: the SMS is displayed in the victim's inbox.
- **Commands**: modifies the trojan's behaviour.

Releasing SMS - those not to spy *(listen - new stuff here)*

Switch to phone's inbox

```
LDR     R0, [R3,#0x34]
MOV     R1, 0x1002  ; KMsvGlobalInboxIndexEntryIdValue
BL      _ZN8CBaseMtm19SwitchCurrentEntryLEl
```

Copy generic information (subject, date) to TMsvEntry object.
Mark the change (CommitL)

```
BL      _ZN5TTime8HomeTimeEv ; TTime::HomeTime(void)
SUB     R3, R11, #0x74
ADD     R0, R3, #0x48
LDR     R1, [R11,#var_1C]
BL      NokiaUpdate_copyTextIfNotNull
...
; CMsvEntry::ChangeL(TMsvEntry  const&)
BL      _ZN9CMsvEntry7ChangeLERK9TMsvEntry
```

Releasing SMS (cont'd)

- Copy message-type specific data (=headers and body) in CMsvStore object.
- Set as `ESmsDeliver` = displayed as coming *from* sender (not *to*)
- Commit.

```
; CSmsHeader::NewL(CSmsPDU::TSmsPDUType,CEditableText &)
MOV     R0, #0 ; ESmsDeliver
LDR     R1, [R11,#var_80]
BL      _ZN10CSmsHeader4NewLEN7CSmsPDU11TSmsPDUType...
...
LDR     R0, [R11,#cmsvstore]
BL      _ZN9CMsvStore7CommitLEv ; CMsvStore::CommitL(void)
```

NB. If listed in the phone's address book, display contact name ("Axelle") and not phone number ("+336...")

Forward SMS to administrator (spy) - *(not 'new', but still listen ;))*

Append Fr: to SMS body

```
; Copy original body in TDes16
LDR     R3, [R11,#var_18]
ADD     R0, R3, #0xC0
LDR     R1, [R11,#incomingsmstext]
BL      _ZN6TDes164CopyERK7TDesC16
; Create TPtrC (pointer) to " Fr:"
SUB     R0, R11, #0x84
LDR     R1, =aFr            ; " Fr:"
BL      _ZN7TPtrC16C1EPKt
; Append " Fr:" to body
SUB     R2, R11, #0x84
LDR     R3, [R11,#var_18]
ADD     R0, R3, #0xC0
MOV     R1, R2
BL      _ZN6TDes166AppendERK7TDesC16
```

Append sender's phone number

```
LDR     R3, [R11,#var_18]
ADD     R0, R3, #0xC0
; phone number in #0x6C
SUB     R3, R11, #0x6C ;
MOV     R1, R3
BL      _ZN6TDes166AppendERK7T
```

- Create SMS in the *Drafts* box.

Dropping an SMS

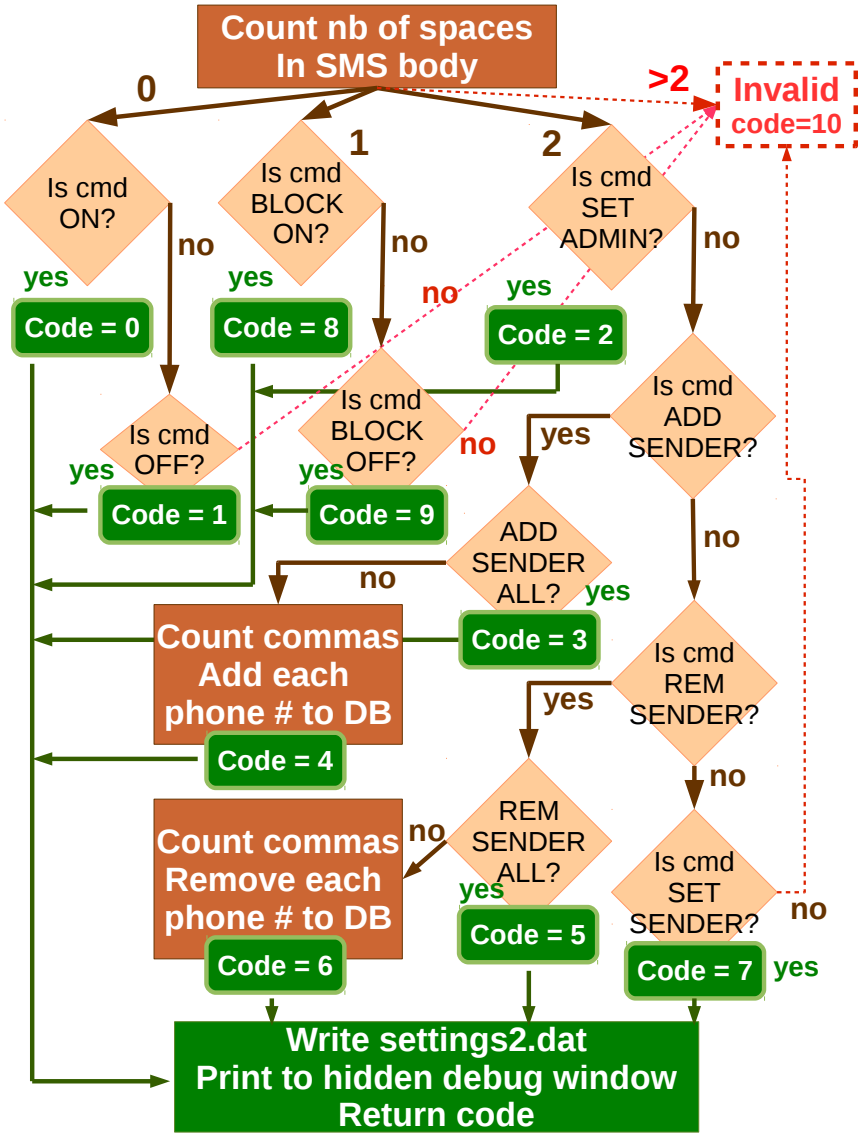
- Do nothing :) ... or nearly:
- Mark SMS PDU as successfully processed (or message re-appears at next boot)

```
; RSocket::Ioctl(uint,TRequestStatus &,TDes8 *,uint)
MOV     R1, #0x304      ; KIoctlReadMessageSucceeded
MOV     R3, R12
BL      _ZN7RSocket5IoctlEjR14TRequestStatusP5TDes8j
```

Zitmo Commands (*listen - new stuff here!*)

- ON / OFF
- SET ADMIN xx
- ADD SENDER xx, xx / ALL
- REM SENDER xx, xx / ALL
- SET SENDER xx
- BLOCK ON / BLOCK OFF

If ALL numbers (except admin) are monitored, SQL tables are not used.
BLOCK ON blocks incoming *calls* (not used)



Zitmo settings file *(listen - new stuff here!)*

- byte 0: state of the trojan: 0 if it is off, 1 if it is on (enabled).
- byte 1: monitoring case: 0 to monitor phone numbers specified in the table, and 1 to monitor any numbers (`ADD SENDER ALL` case).
- byte 2: blocking state: 0 if calls must not be blocked and 1 if they must be blocked (`BLOCK ON/OFF`)
- byte 3-n: externalized 16-bit Unicode string object (`TDesC16`) for the administrator's phone number.

settings2.dat: disabled trojan (OFF), monitor all mode (ADD SENDER ALL), receive incoming calls (BLOCK OFF), admin is +44778148xxxx

```
          00 01 02 03 04 05 06 07  08 09 0a 0b 0c 0d 0e 0f
00000000  00 01 00 34 2b 34 34 37  37 38 31 34 38 x  x  x
00000010  x
```

Spoof administrator (*listen - new stuff here!*)

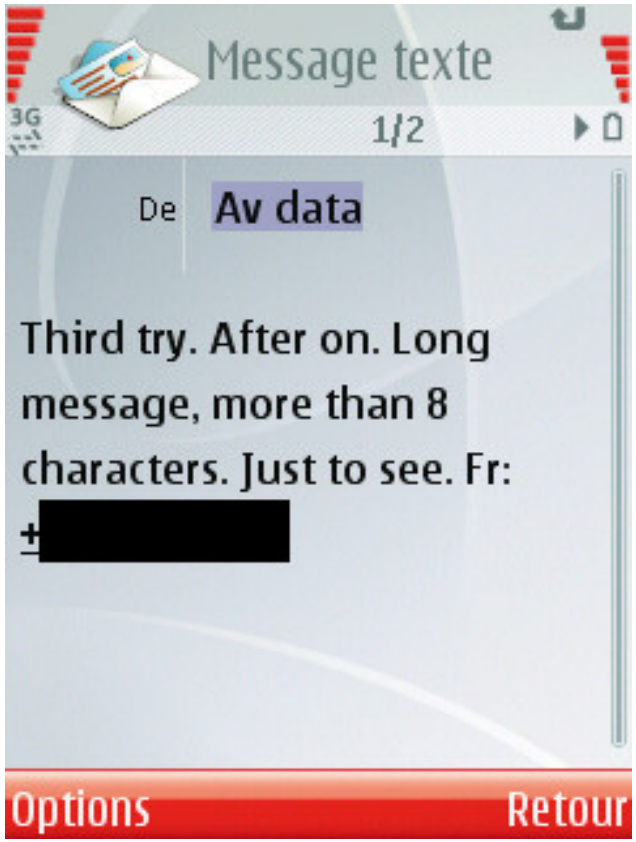
Protocol flaw: *anybody* can claim to be the administrator!

How 0wn the adm1n :D

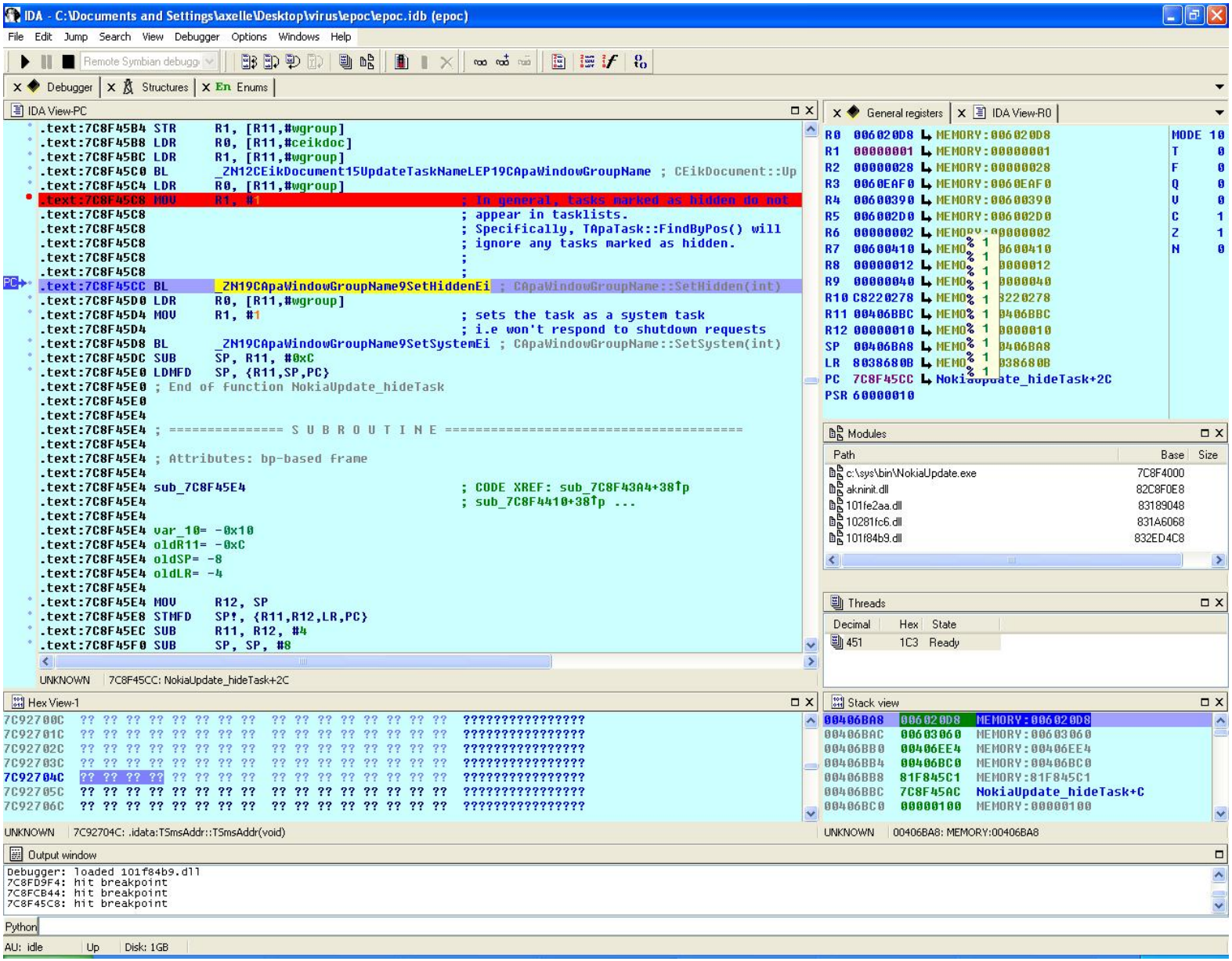
Install Zitmo on lab phone 1

Bonus: make sure it can't send SMS (offline, Faraday cage...)

1. Method 1. Send SET ADMIN command by SMS with phone number of lab phone 2.
2. Method 2. Craft a settings2.dat file with admin phone number = lab phone 2



Remote debugging Symbian phones



Zitmo's Hidden Debug Window (*listen - new stuff here!*)

Un-hide text editor window

CApaWindowGroupName::SetHidden(*EFalse*)

Modify `ETrue=1` to `EFalse=0`.

Bring window in front position

RWindowTreeNode::SetOrdinalPosition(*ECoeWinPriorityAlwaysAtFront*)

Modify `ECoeWinPriorityNeverAtFrom=-1000` or `ECoeWinPriorityNormal=0` to `ECoeWinPriorityAlwaysAtFront=+1000 =0x3e8`

Summary

Overview of Zitmo

Reverse engineering

Conclusion

Zitmo is difficult to spot

Defeating two-factor authentication on demand

Thank You !

Zitmo is difficult to spot

- **Weak symptoms**: alleged certificate packaged as a Symbian package (`.sis`, `.sisx`) not `.p12` or `.pfx`, unknown application listed in the phone's Application Manager
- **Express Signed abused**, but difficult to do really better.

Existing solutions

- Behaviour analysis: Liang Xie and Xinwen Zhang and Jean-Pierre Seifert and Sencun Zhu. *pBMDS: A Behavior-based Malware Detection System for Cellphone Devices*. In WiSec'10, March 2010.
- SMS sending profiles: Guanhua Yan, Stephan Eidenbenz, and Emanuele Galli. *Sms-watchdog: Profiling social behaviors of sms users for anomaly detection*. In RAID, volume 5758 of Lecture Notes in Computer Science, 2009.
- Rules combining security capabilities: William Enck, Machigar Ongtang, and Patrick McDaniel. *On Lightweight Mobile Phone Application Certification*. In CCS'09, November 2009.

Defeating two-factor authentication on demand

Zeus could defeat two-factor authentication before!

True (with a keylogger for example)!
But now, they can do it *when they want*.
No need to wait for the victim to actually login his/her bank.

Possible solution

We need a (secure) hardware device with:

- a keypad
- impossible to install new applications
- communicate result to bank (e.g signed authentication challenge, valid for a given time frame)

Winner (to be improved): a smartcard reader?

Thank You !

Follow us on http://blog.fortinet.com

Axelle Apvrille

aka *Crypto Girl*
/mobile malware reverse engineering/
aapvrille@fortinet.com

Xu (Kyle) Yang

CCIE#19065
/botnet reverse engineering/
xyang@fortinet.com
http://re-malware.com

Thanks to Guillaume Lovet (Fortinet),
David Barroso (s21sec) and Ludovic Apvrille (Telecom ParisTech)

Slides edited with LOBSTER