

*[Seguridad en dispositivos móviles]

Autor: David Barroso

Fecha: 26 de Abril de 2011

Lugar: Madrid, España



Primera pregunta

¿Arquitectura
abierta o cerrada?

Aspectos de seguridad a tener en cuenta

- ⌘ Seguridad física
- ⌘ Cifrado de datos
- ⌘ Autenticación
- ⌘ Safe browsing (exploits o phishing)
- ⌘ Sistema Operativo seguro
- ⌘ Sandboxing (permisos)
- ⌘ Privacidad
- ⌘ **Malware**
- ⌘ Actualizaciones y distribución de paquetes
- ⌘ Notificaciones Push
- ⌘ ¿¿¿¿Enterprise????

Segunda pregunta

¿Recomendaríais un iPad u otro tablet en una empresa?

¿¿Enterprise??

- ⌘ PIN
- ⌘ Borrado remoto
- ⌘ Política de seguridad
- ⌘ Cifrado (FDE, correo, voz, SMS)
- ⌘ Aplicaciones
- ⌘ Redes, VPN
- ⌘ Certificados
- ⌘ **Mobile Device Management (MGM)**
 - Ejemplo: iPhone Configuration Tool

Tercera pregunta

¿Utilizáis AV en
vuestros móviles?

Métodos de infección

⌘ Ingeniería social

⌘ Warez apps

- Black Markets

⌘ Vulnerabilidades o configuraciones débiles (ejemplo Wifi)

The screenshot shows the top portion of the NetworkWorld website. At the top left is the 'NETWORKWORLD' logo in blue and black. To its right are links for 'News', 'Blogs & Columns', 'Subscriptions', 'Videos', and 'Events'. Below this is a blue navigation bar with tabs for 'Security', 'LAN & WAN', 'UC / VoIP', 'Infrastructure Mgmt', 'Wireless', 'Software', and 'Data C'. Underneath the navigation bar is a black bar with links for '3G & 4G', 'Smartphones', 'Mobile Apps', 'Wi-Fi', 'WIMAX & LTE', 'Wireless Management', and 'Wi-Fi Security'. At the bottom of the screenshot is a white box containing a gear icon on the left and a 'Flash' button on the right.

Angry Birds, Monkey Jump apps wrapped with malware

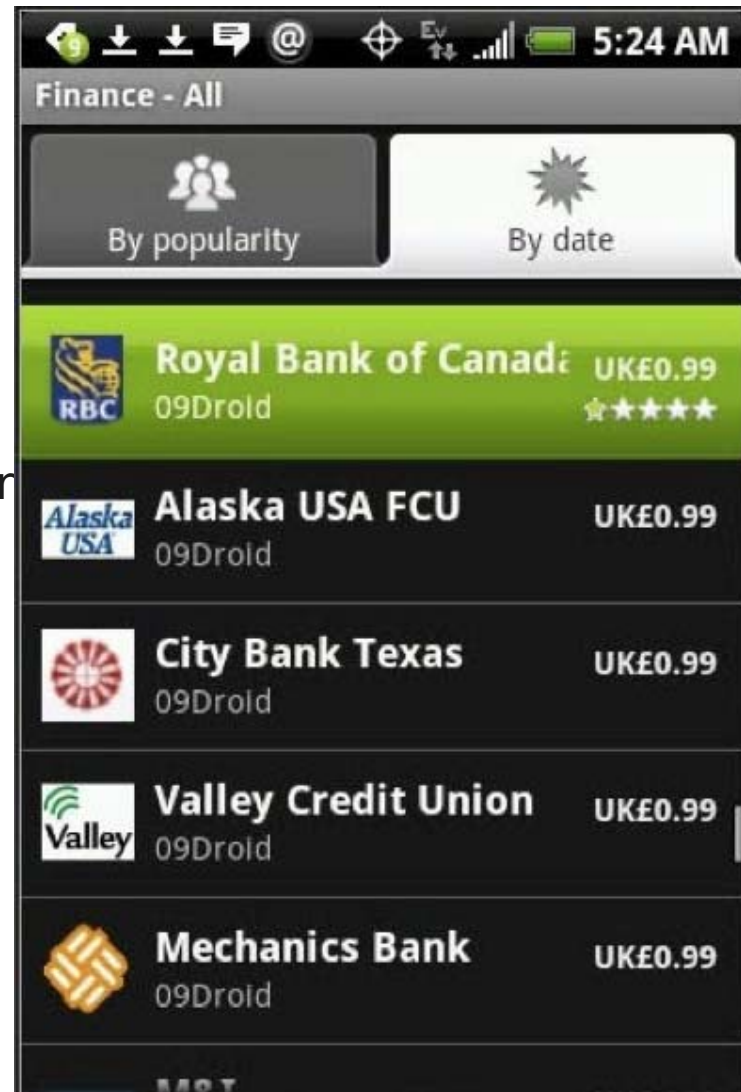
Hackers appear to be increasingly looking for ways to infect mobile devices via applications

By Jeremy Kirk, IDG News Service
February 14, 2011 03:10 PM ET

09Droid

Abbey Bank
Alaska USA FCU
Alliance & Leicester
Bank Atlantic
Bank of America
Bank of Queensland
Barclaycard
Barclays
BB&T
Chase
City Bank Texas
Commerce Bank
Compass Bank
Deutsche Bank
Fifty Third Bank

First Republic Bank
Great Florida Bank
LloydsTSB
M&I Mechanics Bank
MFFCU
MidwestNationwide
NatWest (v. 1.1)
Navy Federal Credit Union
PNC
Royal Bank of Canada
RBS
SunTrust
TD Bank
US Bank
USAA
Valley Credit Union
Wachovia Corp
Wells Fargo



El propio operador

The Register®

Hardware Software Music & Media Networks Security Public Sector Business Science

Crime Malware Enterprise Security Spam ID

 Print  Retweet  Facebook

Alert 

BlackBerry update bursting with spyware

Official snooping suspected in UAE

By [Bill Ray](#) • [Get more from this author](#)

Posted in [Malware](#), [14th July 2009 18:31 GMT](#)

[Free whitepaper – Google Apps: Motorola Case Study](#)

Cuarta pregunta

¿Qué otra persona,
empresa te puede
instalar algo así?

Tu novio/a, pareja, padre, madre, etc.

| | FlexiSpy | MobileSpy | MobiStealth | SpyBubble | TrackWary | Spyera |
|--------------------------|----------|-----------|-------------|-----------|-----------|--------|
| Remote Monitoring | Yes | No | Yes | No | Yes | Yes |
| GPS tracking | Yes | Yes | Yes | Yes | Yes | Yes |
| View Photos | No | Yes | Yes | No | Yes | No |
| Read SMS | Yes | Yes | Yes | Yes | Yes | Yes |
| View call logs | Yes | Yes | Yes | Yes | Yes | Yes |
| Read Email | Yes | Yes | Yes | No | Yes | Yes |
| View Contacts | No | Yes | Yes | Yes | Yes | No |
| View Calendar | No | Yes | Yes | No | Yes | No |
| View Videos | No | Yes | Yes | No | Yes | No |
| BlackBerry Messenger Log | Yes | No | Yes | No | Yes | No |

¿Solución?

ANDROID
developers

Home

SDK

Dev Guide

Reference

Resources

Videos

Blog



Exercising Our Remote Application Removal Feature

Posted by Tim Bray on 23 June 2010 at 10:35 PM

[This post is by Rich Cannings, Android Security Lead. — Tim Bray]

Every now and then, we remove applications from Android Market due to violations of our Android Market [Developer Distribution Agreement](#) or [Content Policy](#). In cases where users may have installed a malicious application that poses a threat, we've also developed technologies and processes to remotely remove an installed application from devices. If an application is removed in this way, users will receive a notification on their phone.

Recently, we became aware of two free applications built by a security researcher for research purposes. These applications intentionally misrepresented their purpose in order to encourage user downloads, but they were not designed to be used maliciously, and did not have permission to access private data — or system resources beyond [permission.INTERNET](#). As the applications were practically useless, most users uninstalled the applications shortly after downloading them.

After the researcher voluntarily removed these applications from Android Market, we decided, per the Android Market [Terms of Service](#), to exercise our remote application removal feature on the remaining installed copies to complete the cleanup.



Quinta pregunta

¿Confíaís en las revisiones que se hacen en las tiendas?

Analicemos el comportamiento

- ⌘ Las herramientas no están tan depuradas como en el mundo Microsoft (IDA rulez! o gdb)
 - Ejemplo: tráfico (tcpdump, o wifi + hub)
- ⌘ Android: dex2jar + jad pero difícil de automatizar (buscar APIs peligrosas)
- ⌘ BlackBerry: casi imposible el reversing
- ⌘ Symbian: ideal el .sisx
- ⌘ Windows Mobile: más sencillo
- ⌘ Hay que familiarizarse con el API de cada plataforma
- ⌘ ARM es nuestra nueva religión

Privacidad

- ⌘ TaintDroid <http://appanalysis.org/demo/index.html>
- ⌘ iPhone Privacy
http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf
- ⌘ iPhone Location Tracking
<http://radar.oreilly.com/2011/04/apple-location-tracking.html>
- ⌘ Skype en Android
http://blogs.skype.com/security/2011/04/privacy_vulnerability_in_skype.html

Ikee Worm

- ⌘ Primer código malicioso para iPhone
- ⌘ Ashley Towns, 21 años
- ⌘ Australia



SSH Scanning

```
116
117 // Entry point.
118 int main(int argc, char *argv[])
119 {
120
121     //pid_t pid, sid;
122     //char *subnet = randHost();
123
124     // syslog(LOG_DEBUG, "I should go, i feel like im interrupting something ;)");
125     /* // FORK CODE REMOVED IT FUCKS WITH LaunchDaemon.
126     pid = fork();
127     if (pid < 0)
128         exit(EXIT_FAILURE);
129     else if (pid > 0)
130         exit(EXIT_SUCCESS);
131
132     umask(0);
133
134     sid = setsid();
135     */
136     if(get_lock() == 0) {
137         syslog(LOG_DEBUG, "I know when im not wanted *sniff*");
138         return 1; } // Already running.
139     sleep(60); // Lets wait for the network to come up 2 MINS
140     syslog(LOG_DEBUG, "IIIIIII Just want to tell you how im feeling");
141     //char ipRange[256] = "120.16.0.0-120.23.255.255";
142     char *locRanges = getAddrRange();
143     char *lanRanges = "192.168.0.0-192.168.255.255"; // #172.16.0.0-172.31.255.255 Ehh who uses it
144     char *vodRanges1 = "202.81.64.0-202.81.79.255";
145     char *vodRanges2 = "23.98.128.0-123.98.143.255";
146     char *vodRanges3 = "120.16.0.0-120.23.255.255";
147     char *optRanges1 = "114.72.0.0-114.75.255.255";
148     char *optRanges2 = "203.2.75.0-203.2.75.255";
149     char *optRanges3 = "210.49.0.0-210.49.255.255";
150     char *optRanges4 = "203.17.140.0-203.17.140.255";
151     char *optRanges5 = "203.17.138.0-203.17.138.255";
152     char *optRanges6 = "211.28.0.0-211.31.255.255";
153     char *telRanges = "58.160.0.0-58.175.255.25";
154     //char *attRanges = "32.0.0.0-32.255.255.255"; // TOO BIG
155
156     syslog(LOG_DEBUG, "awoadqdoqjdajwiodjqoi aaah!");
157     ChangeOnBoot();
158     KillSSHD();
159     // Local first
160     while (1)
161     {
162         syslog(LOG_DEBUG, "Checking out the local scene yo");
163         scanner(locRanges);
164         syslog(LOG_DEBUG, "Random baby");
```

Ikee Worm

☞ Ikee iPhone Worm (alpine):

“<ikee> Secondly I was quite amazed by the number of people who didn't RTFM and change their default passwords.”

☞ Segundo iPhone Worm (ohshit!):

- Roba información
- Es una botnet con dos C&C
- Afecta a bancos holandeses
- Ya no es sólo un script de prueba sino que tiene un proceso malicioso (sshd)

El primer malware 'importante' en Android: Geinimi

⌘ http://blog.mylookout.com/_media/Geinimi_Trojan_Teardown.pdf

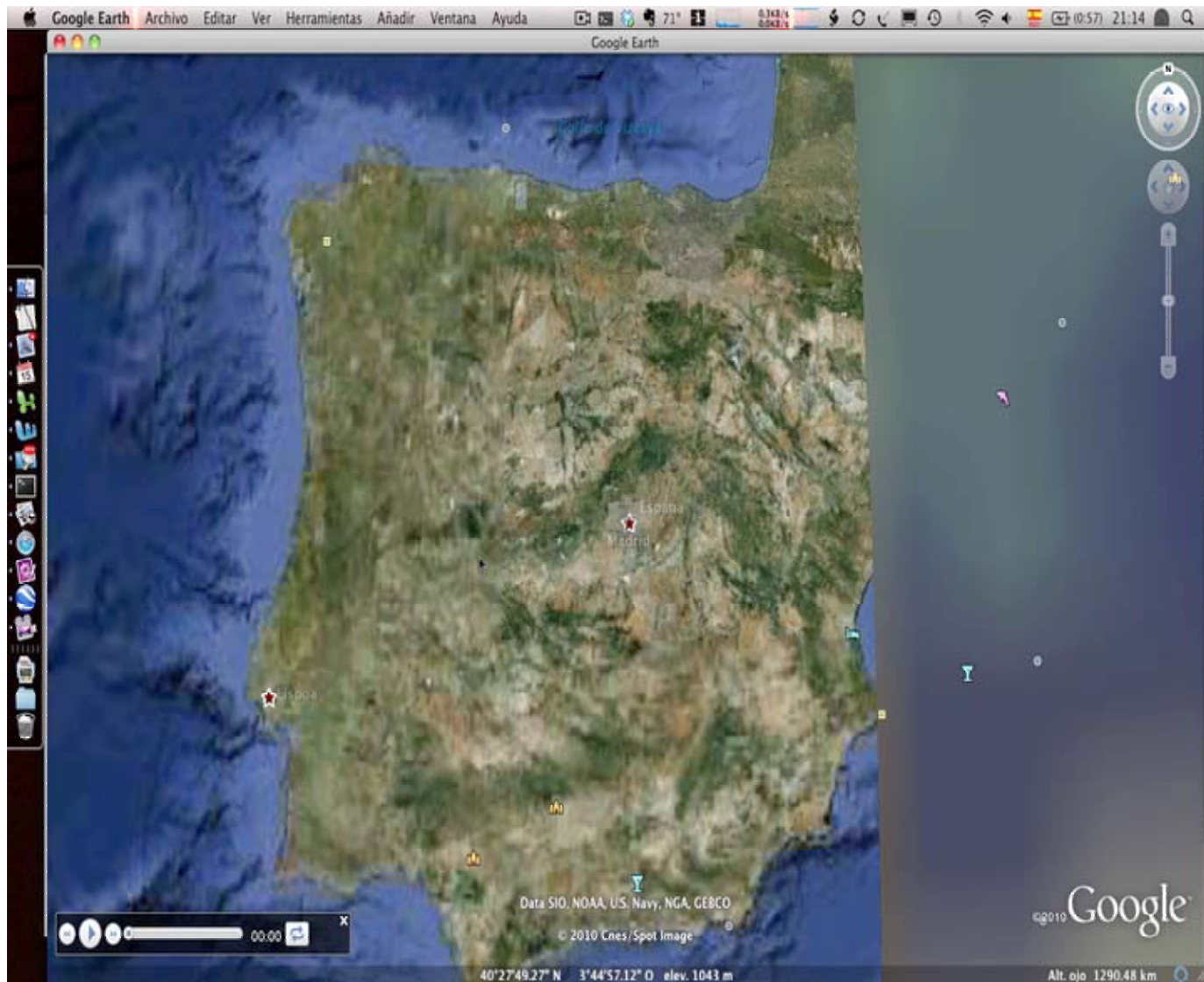
⌘ Cifrado (DES 56 bits) + ofuscación

⌘ Recibe órdenes de un C&C

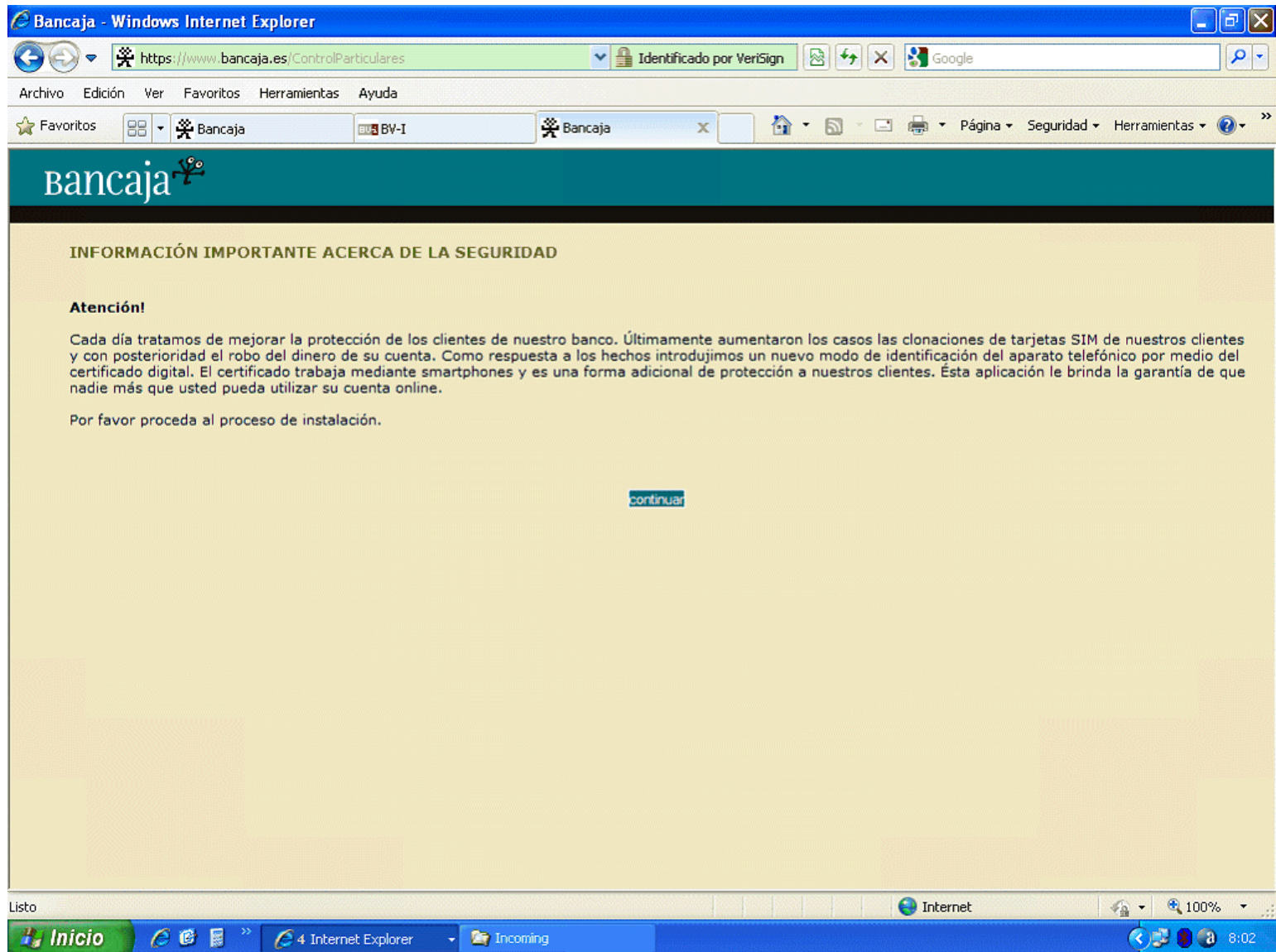
- Borrar SMS
- 'Robar' SMS
- Llamar a un número aleatorio
- Abrir navegador
- Instalar APK
- Listar aplicaciones

El incidente Mitmo

Background



Consiguiendo el teléfono



Bancaja - Windows Internet Explorer

https://www.bancaja.es/ControlParticulares Identificado por VeriSign Google

Archivo Edición Ver Favoritos Herramientas Ayuda

Favoritos Bancaja BV-I Bancaja

Bancaja

INFORMACIÓN IMPORTANTE ACERCA DE LA SEGURIDAD

Atención!

Cada día tratamos de mejorar la protección de los clientes de nuestro banco. Últimamente aumentaron los casos las clonaciones de tarjetas SIM de nuestros clientes y con posterioridad el robo del dinero de su cuenta. Como respuesta a los hechos introducimos un nuevo modo de identificación del aparato telefónico por medio del certificado digital. El certificado trabaja mediante smartphones y es una forma adicional de protección a nuestros clientes. Ésta aplicación le brinda la garantía de que nadie más que usted pueda utilizar su cuenta online.

Por favor proceda al proceso de instalación.

[continuar](#)

Listo Internet 100% 8:02

Consiguiendo el telefono



Bancaja - Windows Internet Explorer

https://www.bancaja.es/ControlParticulares Caja de Ahorros de Valencia Castellon ... Google

Archivo Edición Ver Favoritos Herramientas Ayuda

Favoritos Bancaja BW-I Bancaja Bancaja

bancaja

INFORMACIÓN IMPORTANTE ACERCA DE LA SEGURIDAD

Por favor elija la marca y el modelo de su teléfono

Elijen Elijen

[¿Si el teléfono no existe en la lista?](#)

Su teléfono : -/-

El número de teléfono registrado :

El link para la instalación del certificado móvil digital será enviado al número por SMS, recibido el SMS con el link por favor baje e instale la aplicación.

[continuar](#)

Listo Internet 100%

Conseguiendo el teléfono



Bancaja - Windows Internet Explorer LogMeIn - Sesión remota

https://www.bancaja.es/ControlParticulares Caja de Ahorros de Valencia Castellon ... Google

Archivo Edición Ver Favoritos Herramientas Ayuda

Favoritos Bancaja

Inicio Seguridad Herramientas

Bancaja

INFORMACIÓN IMPORTANTE ACERCA DE LA SEGURIDAD


Por favor elija la marca y el modelo de su teléfono

Nokia 5130 XpressMusic

[¿Si el teléfono no existe en la lista?](#)

Su teléfono : **Nokia 5130 XpressMusic**

El número de teléfono registrado : 608111455

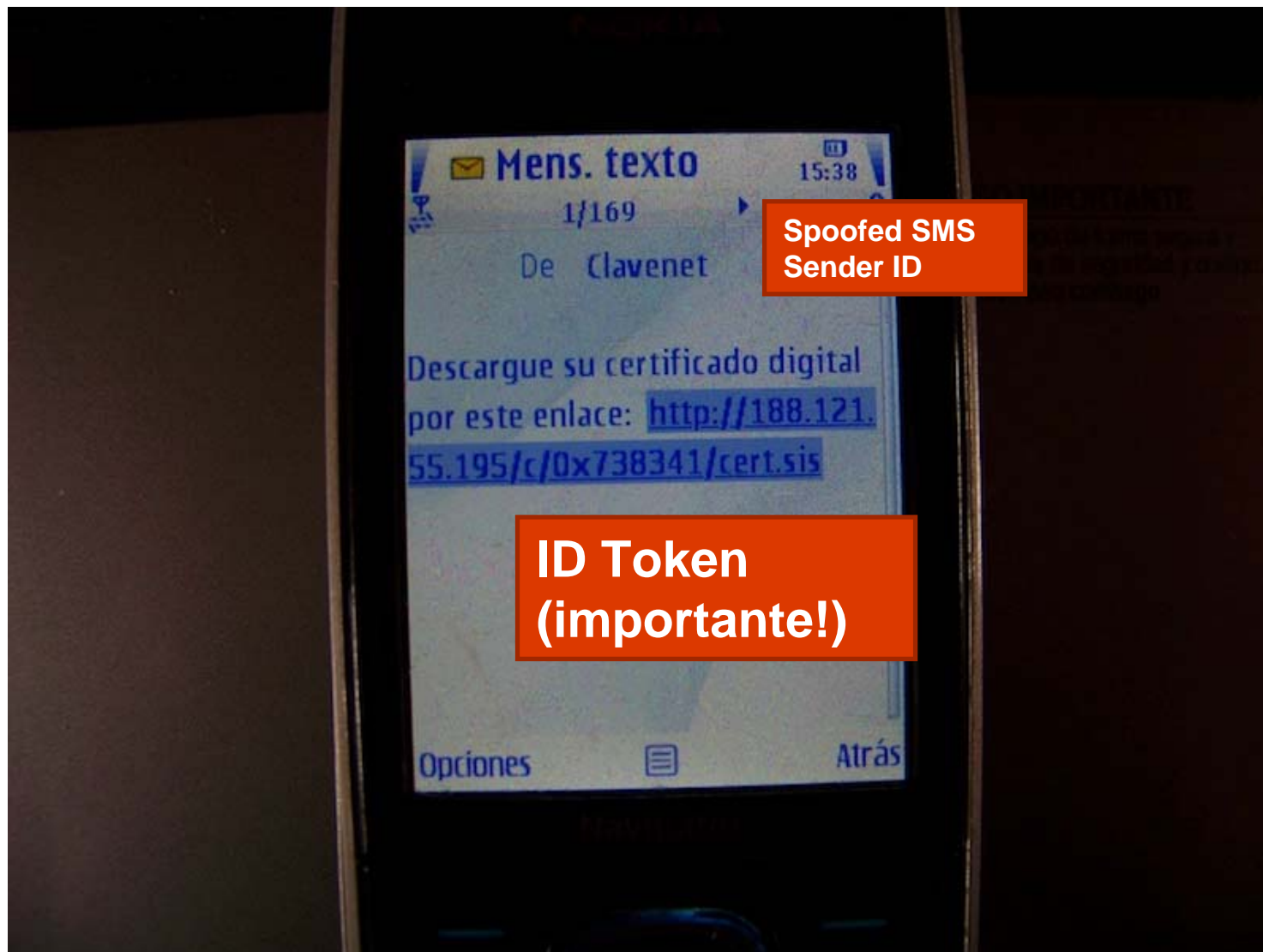


El link para la instalación del certificado móvil digital será enviado al número por SMS, recibido el SMS con el link por favor baje e instale la aplicación.

continuar

Listo Internet 100%

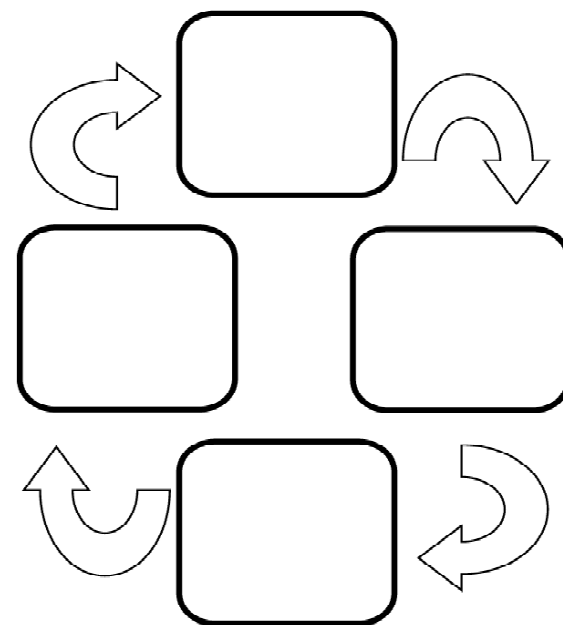
EI SMS



Ciclo de vida del fraude



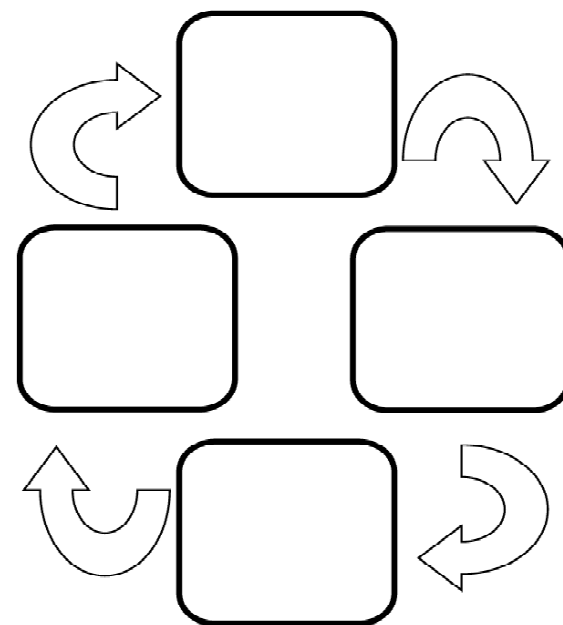
1. Infección del ordenador
2. Robo de credenciales
3. Transferencia fraudulenta
4. Cash out



Ciclo de vida del fraude (actualizada)



1. Infección del ordenador
2. Robo de credenciales
- 3. Infección del móvil**
- 4. Robo OTP-SMS**
5. Transferencia fraudulenta
6. Cash out



ZeuS - Mitmo



- ⌘ El usuario se infecta con ZeuS 2.x
- ⌘ Robo de credenciales
- ⌘ El código inyectado JavaScript pide también la marca, modelo y número de teléfono
- ⌘ El usuario recibe un SMS con un enlace a una aplicación móvil
- ⌘ El usuario instala la aplicación móvil que intercepta los SMS

Zeus Mitmo - Comandos



- ⌘ BLOCK ON: ignora llamadas
- ⌘ BLOCK OFF: deshabilita ignorar
- ⌘ SET ADMIN: cambia el número del C&C SMS
- ⌘ ADD SENDER: añade número a interceptar
- ⌘ ADD SENDER ALL: intercepta todos los SMS
- ⌘ REM SENDER: quita un número a interceptar
- ⌘ REM SENDER ALL: quita toda la interceptación
- ⌘ SET SENDER: actualiza información de un contacto

Zeus Mitmo - Comandos



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 available 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



http://dtarasov.ru/smsmonitor_lite.html

Zeus Mitmo - Certificados



SISContents
File Tools Options Help

E:\Nokia\Data\download\cert.sis **Nokia update** Delete

| | | | |
|----------------|-------------------|---------------------|-------------------------|
| Package UID: | 0x20022B8E | Target devices: | 560 3rd Edition devices |
| Vendor name: | Nokia | Soft. dependencies: | 0 |
| Package name: | Nokia update | Options: | 0 |
| Version: | 1.00(0) | Languages: | UK English |
| Creation date: | 21-09-2010 | Signing status: | Signed |
| Creation time: | 09:49:34 (UTC) | | |
| Install type: | Installation [SA] | | |

Certificate chains (select certificate in the list and click on the right mouse button to see options):

| Issued by | Issued to | Validity |
|--------------|--------------|-------------------------|
| Symbian CA I | Mobil Secway | 21.09.2010 - 21.09.2020 |

Serial Number:

BF43000100230353FF79159EF3B3

**Revocation Date: Sep 28 08:26:26
2010 GMT**

Serial Number:

61F1000100235BC2794380405E52

**Revocation Date: Sep 28 08:26:26
2010 GMT**

| Nombre | Nombre de aplic | Tamaño | Tipo |
|---------------------------|---------------------|---------|-----------|
| YouTube | YouTube | 13 KB | Aplicació |
| SeConUpdater | SeConUpdater | 1 KB | Aplicació |
| App TRK | App TRK | 54 KB | Aplicació |
| Advanced Comm. Man... | Advanced Comm... | 288 KB | Aplicació |
| Ovi Store Client | Ovi Store Client | 283 KB | Aplicació |
| Media DS Plugin | Media DS Plugin | 10 KB | Aplicació |
| Nokia update | Nokia update | 73 KB | Aplicació |
| Metal grey business | Metal grey busin... | 1028... | Aplicació |
| Metal grey personal | Metal grey perso... | 1030... | Aplicació |
| Graphite aluminium bus... | Graphite alumini... | 1078... | Aplicació |
| Graphite aluminium per... | Graphite alumini... | 474 KB | Aplicació |

Espacio disponible en la tarjeta de memoria: 481.8 MB

Respuesta ante incidentes



- ⌘ Bloqueo del envío de SMS al SMS C&C desde todos los operadores
- ⌘ Revocar el certificado de la aplicación móvil (Nokia)
- ⌘ Alerta temprana e informes para clientes
- ⌘ Compartición de binarios entre AV y empresas
- ⌘ Búsqueda activa de otras plataformas (BlackBerry y Windows Mobile)

Windows Mobile



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



Windows Mobile™

Symbian



```
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

BlackBerry



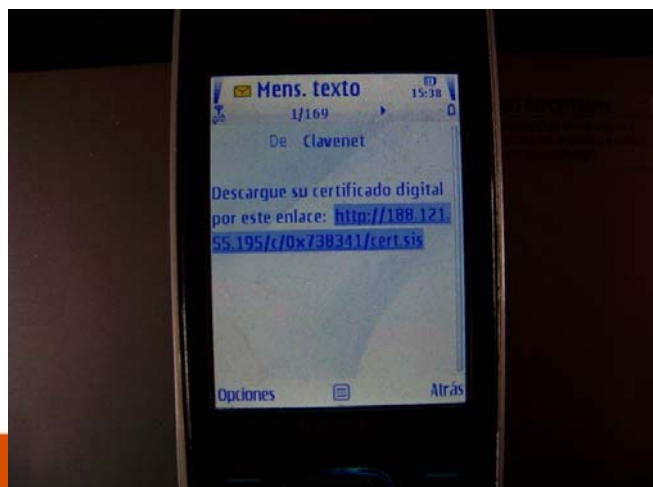
```
if ($urlPathExt == 'cod') {  
$oGate->addHeader('Content-Type: application/vnd.rim.cod');  
if ($data['mobile_os_type'] == OS_BLACKBERRY_41)  
    $oGate->outputFile('./blackberry/cert_41.cod.txt');  
else if ($data['mobile_os_type'] == OS_BLACKBERRY_GR44)  
    $oGate->outputFile('./blackberry/cert_41.cod.txt');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



¿Recuerda el token del SMS?



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





☞ SMS como **autenticación** OOB:

- Si implementa medidas OOB está demostrado que los atacantes intentarán saltárselas (OTP SMS)

☞ SMS como **notificación** OOB:

- Posibilidad de interceptación.

☞ La parte de SMS está muy integrada en el Zeus C&C, y creemos que en las próximas versiones será un plugin.

Conclusiones del incidente



- ⌘ Firmar aplicaciones móviles no sirve de nada si:
 - El fabricante no analiza las aplicaciones
 - No se comprueba el certificado de revocación
- ⌘ ¿Es más fácil perseguir a los atacantes si usan móviles?
- ⌘ El malware para el móvil es ya una realidad (incluso en Android)



🔗 <http://www.youtube.com/watch?v=pNSF1RxzJtg>

Breaking News / Infotech

You are here: Home > News > Breaking News > Infotech

In a Stockholm hotel, mobile phones replace room keys

Agence France-Presse
First Posted 07:30:00 11/03/2010

Filed Under: Computing & Information Technology, mobile phones, Hotels & accommodation

STOCKHOLM—Check-in and check-out and even opening the door to your room – a mobile phone is the only key you need at a Stockholm hotel conducting a pilot project of new mobile applications, the participating companies said Tuesday.

A investigar



- 🌀 Infecciones desde el móvil a un ordenador
- 🌀 Malware multi-plataforma?
- 🌀 NFC
- 🌀 ¿Vuelven los dialers?
- 🌀 ¿Los SMS sirven para más cosas?
- 🌀 Covert channels en nuevos protocolos
- 🌀 IPV6??
- 🌀 In-game purchases
- 🌀 Localización por Wifi, GPS, celda, 4square
- 🌀 ¿Qué pasó con Bluetooth?

***[MUCHAS GRACIAS]**

David Barroso

S21sec e-crime Director

dbarroso@s21sec.com

<http://blog.s21sec.com>



lostinsecurity

 **S21sec** university

www.s21sec.com
info@s21sec.com
+34 902 222 521

