

Cómo se hizo: El bueno, el feo y el malo

Raúl Siles
DinoSec



www.incibe.es

INSTITUTO NACIONAL DE
CIBERSEGURIDAD
SPANISH NATIONAL
CYBERSECURITY INSTITUTE



<https://cybercamp.es>

#CyberCamp15





www.dinosec.com
[@dinosec](mailto:raul@dinosec.com)

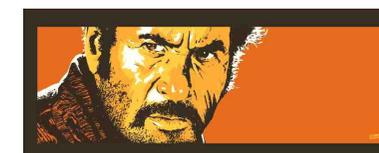
Raúl Siles

raul@dinosec.com





THE GOOD THE BAD AND THE UGLY

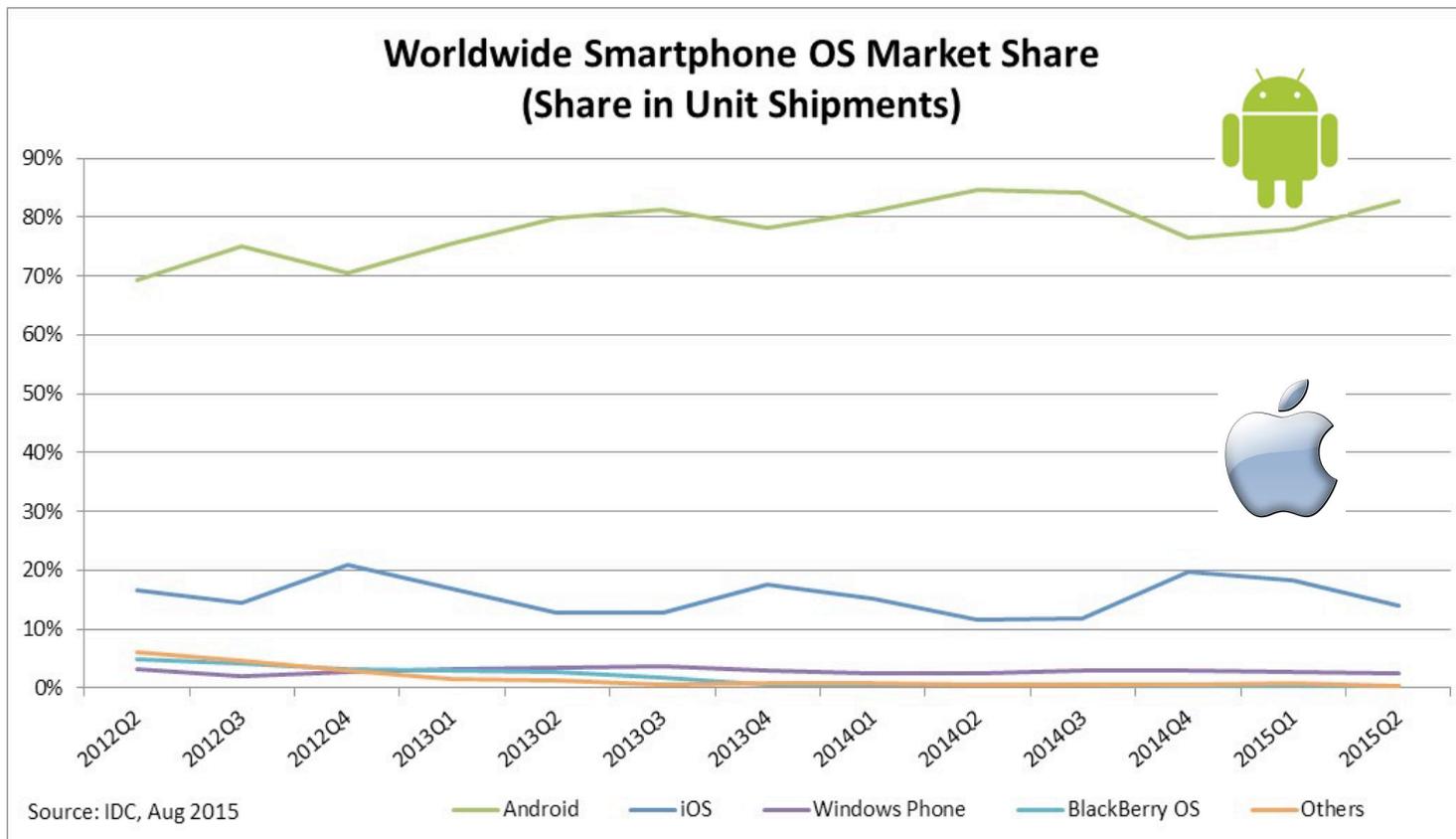


El bueno, el feo y el malo

- **Los dispositivos y entornos móviles son un objetivo y están constantemente amenazados por...**
 - Comportamientos del usuario arriesgados...
 - ... pero muy habituales
 - Integración con la plataforma del fabricante
 - Apple, Google, Microsoft...
 - Vulnerabilidades de seguridad
 - La importancia de las actualizaciones



Cuota de mercado de los dispositivos móviles



Q2 2015:

- ▶ Android: 82.8%
- ▶ iOS: 13.9%
- ▶ WP: 2.6%
- ▶ BB: 0.3%
- ▶ Others: 0.4%

Tendencia consolidada a sobrepasar 300 millones de unidades por trimestre (Qx): 1,3b (2014)

Referencia: <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>

El bueno...



El bueno...

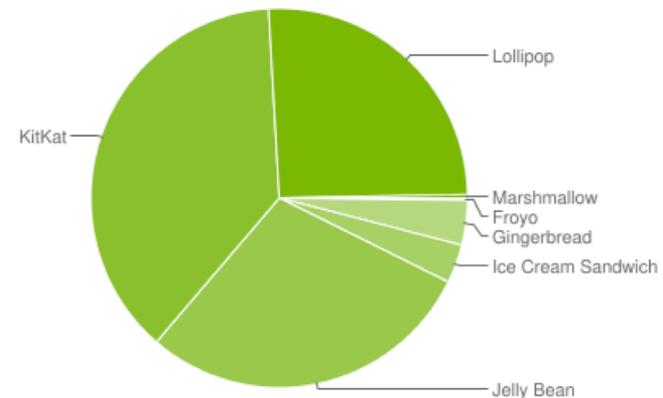


- **¿Disponéis de la última versión del sistema operativo para vuestro dispositivo móvil?**
- **¿Siempre... (tan pronto es publicada)?**
 - Si es que es publicada para vuestro modelo de dispositivo móvil
- **La última versión soluciona todas las vulnerabilidades de seguridad conocidas**
 - ¿Seguro...?
 - ¿...y entre actualizaciones?
 - ¿...y las vulnerabilidades que no son públicas?

Distribución de versiones de Android

- **Noviembre de 2015:** <https://developer.android.com/about/dashboards/index.html>

Version	Codename	API	Distribution
2.2	Froyo	8	0.2%
2.3.3 - 2.3.7	Gingerbread	10	3.8%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	3.3%
4.1.x	Jelly Bean	16	11.0%
4.2.x		17	13.9%
4.3		18	4.1%
4.4	KitKat	19	37.8%
5.0	Lollipop	21	15.5%
5.1		22	10.1%
6.0	Marshmallow	23	0.3%



Vulnerabilidad
Towelroot:

≈ 38%... (≈ 75%)

Ritmo al que consumimos la tecnología: Android



■ Android: 8 años

- 2008: 1.0
- 2009: 1.1 & 1.5 & 1.6 & 2.0
- 2010: 2.1 & 2.2 & 2.3.x
- 2011: 2.3.x & 3.x & 4.0
- 2012: 4.1 & 4.2
- 2013: 4.3 & 4.4
- 2014: 5.0
- 2015: 5.1 & 6.0

Nº. oficial de vulnerabilidades:

Desconocido...
(hasta Agosto 2015
para móviles Nexus)

Nº. oficial de vulnerabilidades:

- Ago 15: 6
- Sep 15: 9
- Oct 15: 30
- Nov 15: 7

Android - Total: 52



Ritmo al que consumimos la tecnología: iOS



■ iOS: 9 años

- 2007: iPhone 2G (iOS 1)
- 2008: iPhone 3G (iOS 2)
- 2009: iPhone 3GS (iOS 3)
- 2010: iPhone 4 (iOS 4) + iPad 1
- 2011: iPhone 4S (iOS 5) + iPad 2
- 2012: iPhone 5 (iOS 6) + iPad 3 & 4 & mini
- 2013: iPhone 5c & 5s (iOS 7) + iPad air & mini 2
- 2014: iPhone 6 & 6+ (iOS 8) + iPad air 2 & mini 3
- 2015: Apple Watch (1 & 2) & iOS 9



Nº. oficial de vulnerabilidades:

- iOS 6: 197
- iOS 7: 80
- iOS 7.1: 41
- ...

Nº. oficial de vulnerabilidades:

- iOS 8: 56
- iOS 8.1: 5
- iOS 8.1.1: 9
- iOS 8.1.2: -
- iOS 8.1.3: 34
- iOS 8.2: 6
- iOS 8.3: 58
- iOS 8.4: 33
- iOS 8.4.1: 71

iOS 8.x: 272

Nº. oficial de vulnerabilidades:

- iOS 9: 101
- iOS 9.0.1: -
- iOS 9.0.2: 1
- iOS 9.1: 49

iOS 9.x: 151

El feo...



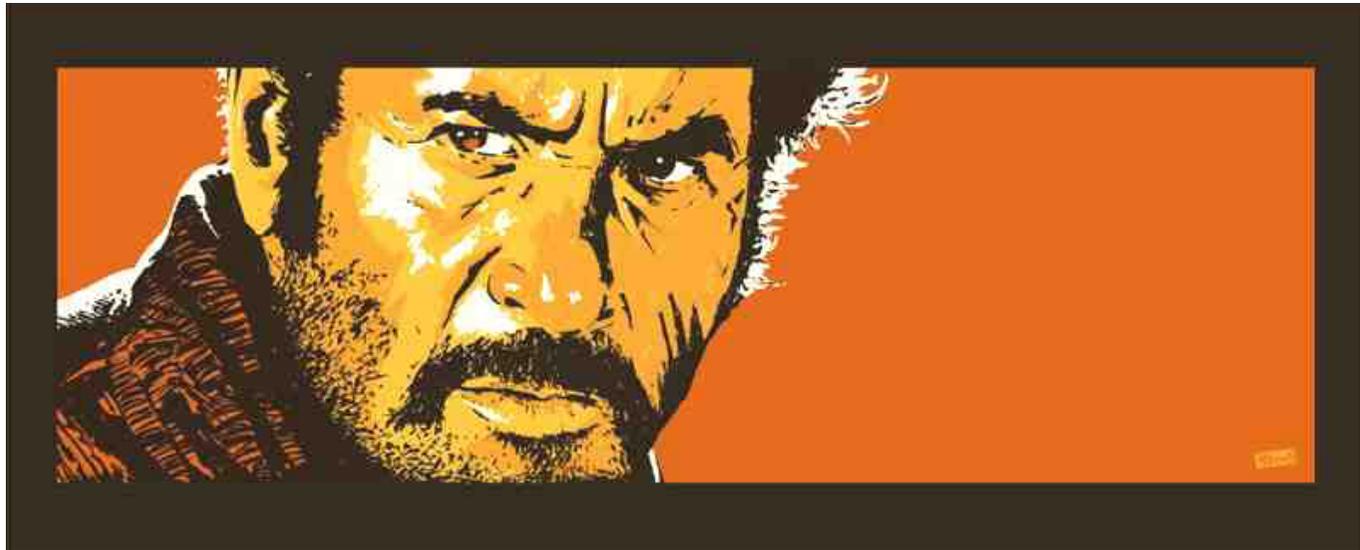
El feo...



- **¿Tenéis cuenta de usuario en la plataforma del fabricante del dispositivo móvil?**
 - Apple, Google, Microsoft, etc
- **¿Cuándo la creásteis?**
 - Proceso de instalación y ¿compras?
- **¿Vuestro usuario es conocido?**
 - E-mail
- **La contraseña es robusta, ¿verdad?**
 - Y no la reutilizáis entre distintos servicios...



... el malo



... el malo



- ¿Qué hace que los teléfonos móviles actuales sean inteligentes: *smartphones*?
- ¿Instaláis aplicaciones móviles (apps) en vuestros dispositivos móviles?
- ¿Para qué...? (uso profesional, personal...)
- ¿De quién...? (terceros)
 - Mercados (oficiales, 3^{os}...) & desarrolladores
- ¿Con qué criterio...? (reputación)

Mercados oficiales de apps

■ App Store, Google Play, etc

- 2015:
- ¿1,5 millones?
- ¿100,000 millones?

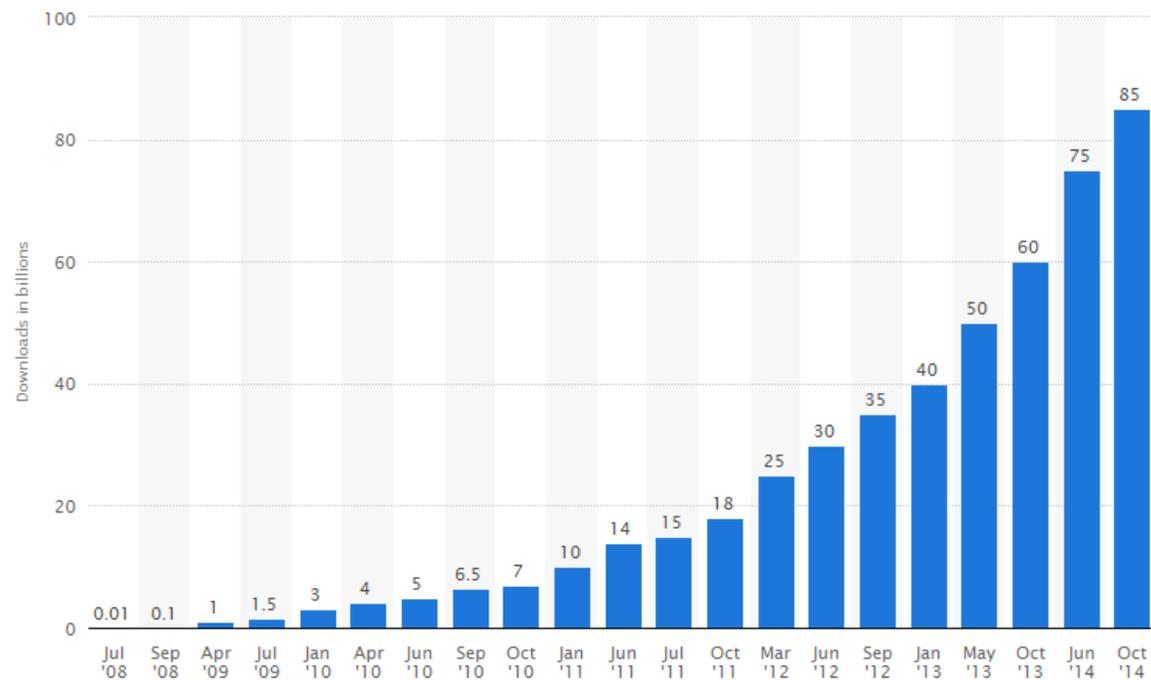


Available on the
App Store



Get it on
Google play

Google play



“Malware” móvil: DroidScale



Debéis acuñar
vuestra propia
definición de
“malware” móvil.

DroidScale (1/3)



DroidScale
DroidMob Technologies - December 21, 2009
Tools Tools

[Install](#) [Add to Wishlist](#)

This app is compatible with all of your devices.

★★★★☆ (6,515) [g+1](#) +1180 [Recommend this on Google](#)



Description

OVER 1 MILLION DOWNLOADS!!!! AD FREE PRO VERSION ALSO AVAILABLE!

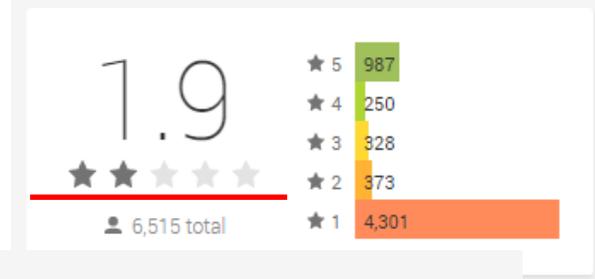
This dynamic app turns your phone into a digital scale that you can take with you wherever you go!

Weigh normal household items with your friends, and see who can get the closest guess! Weighs in grams or ounces!

Follow the in-app instructions for use.

Note: DroidScale does not guarantee exact measurements.

Reviews

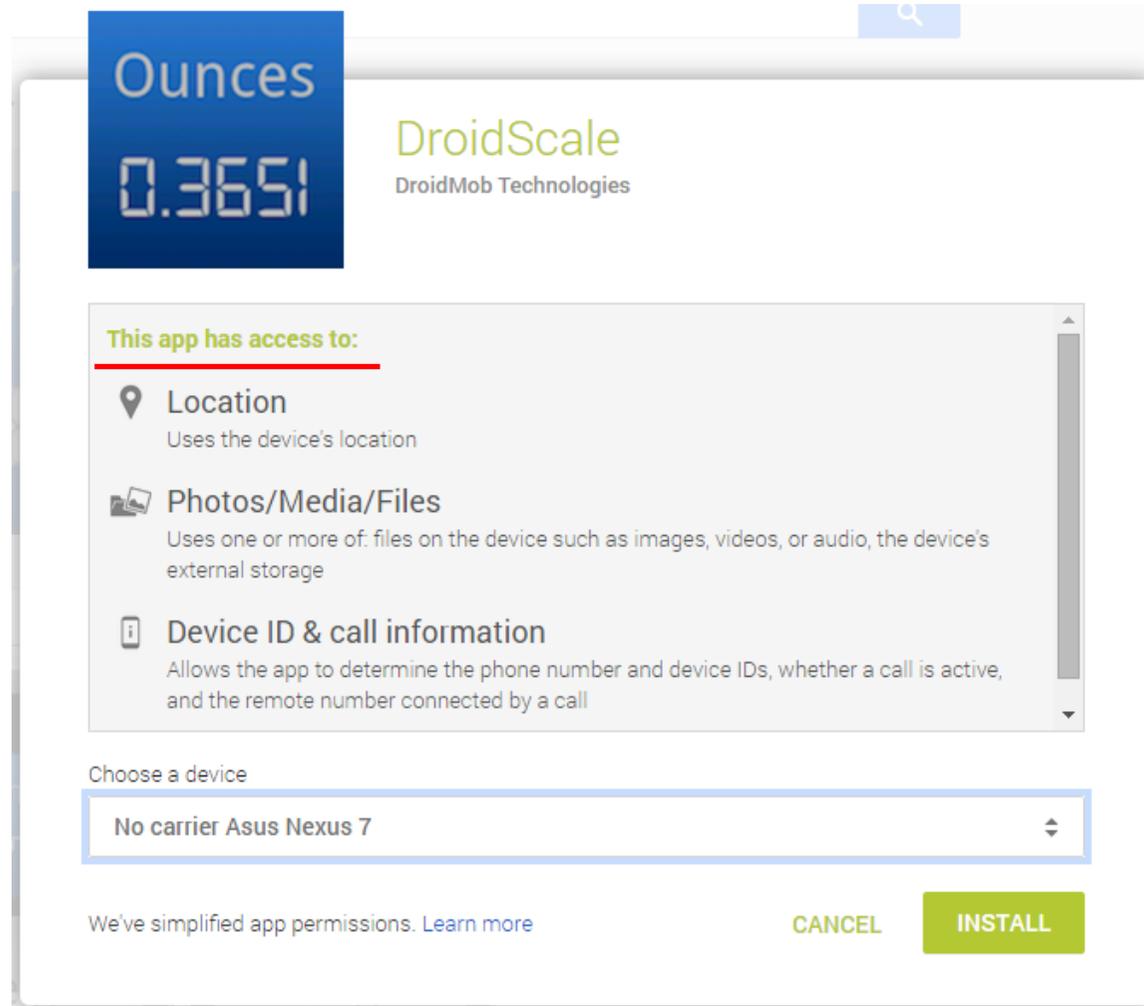


Additional information

Updated December 21, 2009	Size 155k	Installs <u>1,000,000 - 5,000,000</u>	Current Version 1.0	Requires Android 1.1 and up	Content Rating Low Maturity
Contact Developer Email Developer	Permissions View details	Report Flag as inappropriate			



DroidScale (2/3)



DroidScale (3/3)

```
153 public void onCreate(Bundle paramBundle)
154 {
155     super.onCreate(paramBundle);
156     rgen = new Random();
157     curr = 0.0D;
158     conversion = 28.3495231D;
159     new AlertDialog.Builder(this).setMessage("Warning: DroidScale is intended for lightweight ob
jects and will not accurately display heavy weights. Do not place too much weight on the scale f
or the safety of your screen! \n \nPlace a finger on the scale and place the object you desire t
o weigh on top of your finger.").setPositiveButton("OK", null).setTitle("Instructions").setIcon(
0).show();
160     TextView localTextView = (TextView)findViewById(R.id.units);
161     localView.setOnTouchListener(new View.OnTouchListener()
162     {
163         public boolean onTouch(View paramAnonymousView, MotionEvent paramAnonymousMotionEvent)
164         {
165             if (paramAnonymousMotionEvent.getAction() == 1)
166             {
167                 touchDown = false;
168                 curr = 0.0D;
169                 masterTextView.setText("0.0000");
170                 return true;
171             }
172             for (curr = rgen.nextDouble(); curr = rgen.nextDouble()) {
173                 if (curr >= 0.2D)
174                 {
175                     if (inGrams)
176                     {
177                         DroidScale localDroidScale = DroidScale.this;
178                         curr *= conversion;
179                     }
180                     String str = Double.toString(curr).substring(0, 6);
181                     masterTextView.setText(str);
182                     touchDown = true;
183                     fluctuateWeights();
184                     return true;

```

Referencia: <http://viemot.com/playdrone-slides.pdf>



DroidScale Pro (1/2)

Description

★★★★★ AD FREE AND OPTIMIZED! OVER 1 MILLION DOWNLOADS OF THE AD SUPPORTED VERSION! REDUCED INTRODUCTORY PRICE! ★★★★★
The ads have been removed to give you a better experience with more available screen space to weigh your items! The previous ad supported version had over a million downloads and the demand was growing, so the application has been upgraded and optimized in order to give you a better experience!

This dynamic app turns your phone into a digital scale that you can take with you wherever you go!
Weigh normal household items with your friends, and see who can get the closest guess! Weighs in grams or ounces!
Follow the in-app instructions for use.

Note: DroidScale does not guarantee exact measurements.

Reviews

2.8

★ 5	8
★ 4	3
★ 3	2
★ 2	0
★ 1	12

25 total

DroidScale Pro
DroidMob Technologies - August 17, 2011
Tools Tools

€0.69 Buy Add to Wishlist

This app is compatible with all of your devices.

★★★★★ (25) **8+1** +112 Recommend this on Google

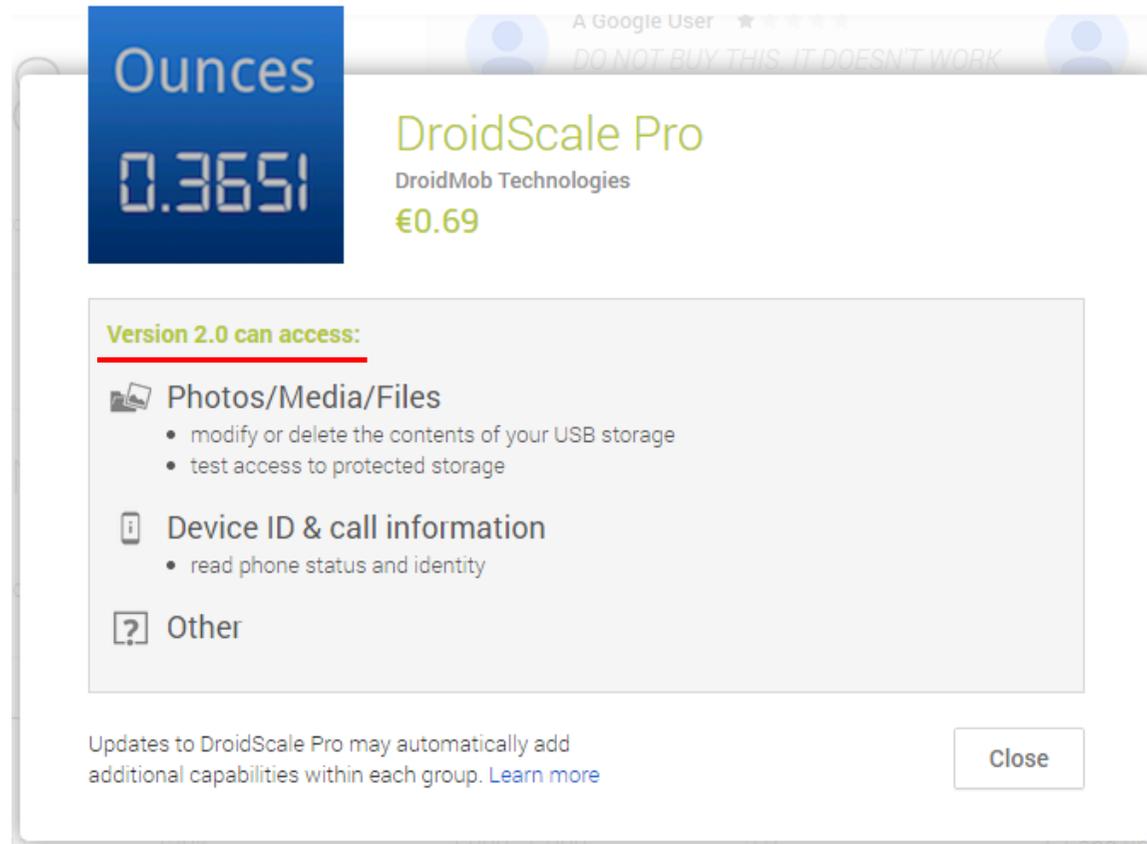
Installs
1,000 - 5,000

Current Version
2.0

Report
[Flag as inappropriate](#)

cyber camp

DroidScale Pro (2/2)



A screenshot of the Google Play Store page for the app "DroidScale Pro" by DroidMob Technologies. The page shows the app's name, developer, price (€0.69), and a list of permissions. A blue box on the left displays the word "Ounces" and the number "0.3651". The permissions are listed under the heading "Version 2.0 can access:" and include "Photos/Media/Files", "Device ID & call information", and "Other". A "Close" button is visible at the bottom right of the page.

Ounces
0.3651

DroidScale Pro
DroidMob Technologies
€0.69

Version 2.0 can access:

- Photos/Media/Files**
 - modify or delete the contents of your USB storage
 - test access to protected storage
- Device ID & call information**
 - read phone status and identity
- Other**

Updates to DroidScale Pro may automatically add additional capabilities within each group. [Learn more](#)

Close

¡Error!



¿Debemos proteger al móvil del usuario?



This is the watermark of **FAILKING.COM**



Y U NO go to **FAILKING.COM**

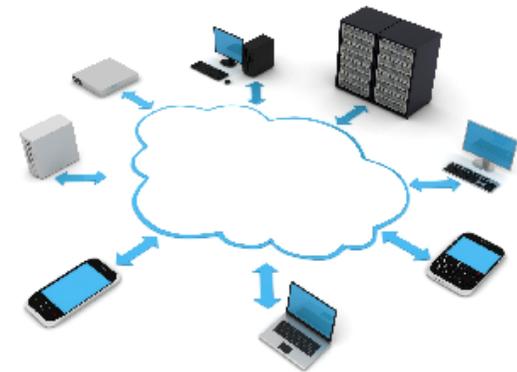


Conclusiones

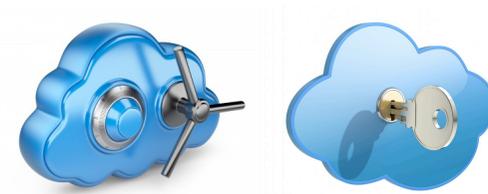


Protege tu vida digital

- **Dispositivos móviles = Cuenta usuario (credenciales) = Usuario (datos...)**



Riesgo de seguridad móviles



■ Exfiltración de datos e información confidencial

- Contenida en el dispositivo móvil
 - Documentos, fotos, ficheros descargados, correos, SMS, registro de llamadas, contactos, geolocalización, WhatsApp y mensajería, redes sociales (privadas)...
 - Contraseña(s) de la red(es) Wi-Fi, código de acceso, patrón de desbloqueo, (gestor de) contraseñas...
- Credenciales...de acceso a múltiples servicios
 - Internet, “en la nube”, VPN, casa, red interna de la organización...
 - E-mail, aplicaciones web, servicios de almacenamiento de ficheros...
- Ransomware: exfiltración + extorsión, chantaje, DoS...

Recomendaciones

- **Instalar aplicaciones móviles (apps) sólo de los mercados oficiales**
 - Google Play (Android), App Store (iOS), Marketplace (WP)...
 - Verificar su reputación
 - Android: No aceptar apps de “Orígenes desconocidos” (y “Verificar aplicaciones”)
- **Selección cuidadosa de las credenciales de usuario: robustas**
- **No realizar el proceso de jailbreak o root**
- **Actualizar los dispositivos móviles a la última versión (...)**
- **Concienciación de los usuarios con menos...**
 - ¿Conocimientos técnicos...? o criterio y experiencia
- **Apps gratuitas: “Si no estás pagando... tú eres el producto”**
- **Implementar una solución de gestión empresarial de dispositivos móviles (*MDM, Mobile Device Management*)**
 - MDM, MAM, MCM... (MEM): Listas blancas de apps verificadas y aprobadas



Preguntas





<https://cybercamp.es>

[#CyberCamp15](https://twitter.com/CyberCampEs)

[@CyberCampEs](https://twitter.com/CyberCampEs)

