Identificando amenzas en tu móvil

Leonardo Huertas Calle
CSA – Chief Security Ambassador at 11Paths
leonardo.huertas@11paths.com
@SamuraiBlanco

A Telefónica COMPANY

¿Dónde está implementada la movilidad?

¿Qué contienen las aplicaciones móviles?

Short link

http://d.pr/i/1ikxR/iFY2qhBx44s

Password

INSECURE

Figure 3. Vulnerability marketplace options

Jailbreak?
Rootear?
Es riesgoso?

Ciberseguridad y movilidad

- Existe una necesidad de conectividad tanto a nivel personal como corporativo.

- **A mayor nivel de interconexión, mayor es el número de amenazas que afectan a todo el ecosistema móvil.**

Panorama de amenazas móviles

Más de 2.000 millones de smartphones en el mundo (2014)

Android representa el 81% de la cuota de mercado de sistemas operativos móviles

El número de troyanos bancarios en apps es 9 veces superior que en 2014 :'(

Con más de 1.000 millones de dispositivos, Android es el foco del 96% de los ciberataques móviles

Se estima cerca de 15 millones de dispositivos están infectados, con un crecimiento 36% YoY

Ciberseguridad y movilidad

Amenazas y riesgos existentes

Las amenazas de seguridad en entornos Android están basadas mayoritariamente en cepas de malware cada vez más sofisticadas, así como en vulnerabilidades del sistema operativo, poniendo los datos corporativos en situación de riesgo

Las aplicaciones móviles maliciosas son un fenómeno real y creciente

Eleven Paths

Es necesario aplicar inteligencia de aplicaciones móviles?

Facilitar la investigación en entornos de aplicaciones móviles mediante tecnología de big data a CSIRTs, compañías, organismos de seguridad, profesionales expertos en seguridad.

Búsqueda en tiempo real de información de amenazas móviles

Analizar y comprender las amenazas móviles

Detectar y correlacionar/correlar campañas de amenazas móviles

Creación de perfiles de atacantes atendiendo a su modus operandi.

Alerta temprana de nuevas amenazas móviles

Con un poco de investigación, un desarrollador malicioso puede ser identificado

Algunas capacidades para la vigilancia, detección e investigación de amenazas en los entornos de aplicaciones móviles.

02

La diversidad de markets de aplicaciones móviles dificulta el control de la seguridad de nuestros dispositivos?

Ejemplo de cómo un investigador podría identificar amenazas en un market móvil

tacyt : THE TOOL FOR APP CYBER INTELLIGENCE

Language ca[redacted]

- Search
- Comparer
- Filters
- My tags
- APK upload
- My APIs
- Help

Search

title:*Farm*

Order by: Relevants first

Search

4,511 results found, **858** (**19.02%**) of them are now unavailable apps in their markets

Farm Heroes Saga (Version 223031 in Google Play)

King | farmheroesmobile@support.king.com | Cristian Bidea

New and improved Farm Club available now! From the makers of the hit game Candy Crush Saga, comes Farm Heroes Saga! Switch and match the collectable cropsies in this fantastic adventure. Join forces with the Farm Heroes to stop Rancid the Raccoon from spoiling the precious farm lands. Switch and ...

Farm Heroes Saga (Version 220041 in Google Play)

King | farmheroesmobile@support.king.com | Cristian Bidea

New and improved Farm Club available now! From the makers of the hit game Candy Crush Saga, comes Farm Heroes Saga! Switch and match the collectable cropsies in this fantastic adventure. Join forces with the Farm Heroes to stop Rancid the Raccoon from spoiling the precious farm lands. Switch and ...

Telefónica

tacyt : THE TOOL FOR APP CYBER INTELLIGENCE

Language ca[redacted]

- Search
- Comparer
- Filters
- My tags
- APK upload
- My APIs
- Help

Search

title:*Farm* deadDate:*

Order by: Relevants first

Search

858 results found, **858** (**100.00%**) of them are now unavailable apps in their markets

Tiny Farm® (Version 160)

2014-09-29 14:03:37

Com2uS USA | support@com2us.com | Com2us

For a farm so small it fits in your hands, Tiny Farm is jam-packed with sweet surprises and endless possibilities! ★ Recommended as most interesting Virtual game by AppEggs! ★ ★ Recommended as top 10 hottest app by AppBrain! ★ * Tiny Farm is packed with the rarest animals(115MB+). WiFi connection is ...

Tiny Farm® (Version 158)

2014-09-29 08:10:29

Com2uS USA | support@com2us.com | Com2us

For a farm so small it fits in your hands, Tiny Farm is jam-packed with sweet surprises and endless possibilities! ★ Recommended as most interesting Virtual game by AppEggs! ★ ★ Recommended as top 10 hottest app by AppBrain! ★ * Tiny Farm is packed with the rarest animals(115MB+). WiFi connection is ...

Telefónica

tacyt : THE TOOL FOR APP CYBER INTELLIGENCE

Language [redacted]

- Search
- Comparer
- Filters
- My tags
- APK upload
- My APIs
- Help

Search

title:*Farm* deadDate:* links:*.apk

Order by: Relevants first

Search

4 results found, **4** (**100.00%**) of them are now unavailable apps in their markets

Sheep Farm Theme GO Locker (Version 6)

2015-03-17 13:25:00

zwoodle design | zwoodledesign@hotmail.com | Unknown

Sheep Farm Theme for GO Locker --- zwoodle design --- Get a lovely sheep on your locker screen! You need GO Launcher EX and GO Locker to use this theme. Sheep Farm Theme for GO Locker is also a perfect addition to my "Sheep Farm Theme" for GO Launcher EX which you can download on Google Play. :) ...

Farm Quest (Version 21)

2015-04-17 02:22:05

Sigma Game | apps@superapk.com | Sigma

Happy farming! Happy collecting fruits and vegetables or farm animals on the farm Quest. Connected to the same fruits and vegetables or farm animals, will be able to collect the elimination of classes, complete all levels of the game modes, and try to get three vegetable stars. Come Quest farm happy ...

Telefónica

tacyt : THE TOOL FOR APP CYBER INTELLIGENCE

Language [redacted]

Farmer Keyboard (Version 3)

2015-04-15 18:51:14

Themes World | themesonlyex@gmail.com | TMe CEO

Life at a farm is just so much more simple than the city life so we prepared this theme for the simple life: FARMER K EYBOARD! DOWNLOAD Farmer Keyboard NOW and take it easy with these beautiful graphics! - To install, just follow the 3 steps: open after downloading, press "Set as Active Theme" and ...

Farm Splash Heroes (Version 1)

2015-05-20 00:03:11

Heroes Game | wzglabc@gmail.com | felix

Harvest season, happy farm, a variety of fruits and vegetables get together and throw a huge party.Come on,let's da nce and tango,let us enjoy the crazy elimination. Joy carrots, arrogant green apple, melancholy small mushrooms, s weet purple onions, shy tomatoes, naughty warters and so on. All show ...

2015 © ElevenPaths. All Rights Reserved.

Telefónica

tacyt : THE TOOL FOR APP CYBER INTELLIGENCE

Language ca[redacted]

- Search
- Comparer
- Filters
- My tags
- APK upload
- My APIs
- Help

Farm Splash Heroes

Download app

General information

Add Tags

Origin	GooglePlay
Category	GAME_PUZZLE
Size	14,890,663 bytes
Number of downloads	100
Version code	1

Telefónica

tacyt : THE TOOL FOR APP CYBER INTELLIGENCE

Language [redacted]

Add Tags

http://shouji.360tpcdn.com/140714/26c2fd446feccb287e4444483d025bf6/com.goodlogic.chickensplash_2.apk

http://media.admob.com/mraid/v1/mraid_app_banner.js

http://xmlpull.org/v1/doc/features.html#indent

http://nfrkfw.com/goodlogic/moregames/newgameJellycrushsaga.png

https://api.weibo.com/2/statuses/update.json

https://api.weibo.com/2/friendships/create.json

http://plus.google.com/

https://api.weibo.com/2/friendships/friends.json

https://api.weibo.com/oauth2/access_token

http://commons.apache.org/logging/troubleshooting.html.

https://graph.facebook.com/

http://hostname/?

https://graph.facebook.com/me/feed

https://graph.facebook.com/me/photos

https://api.weibo.com/2/statuses/user_timeline.json

http://api2.sharesdk.cn:5566

http://nfrkfw.com/goodlogic/apk/jellycrushsaga.apk

https://twitter.com/

http://sites.google.com/site/gson/gson

http://schemas.android.com/apk/lib/com.google.android.gms.plus

http://api2.sharesdk.cn:5566/conf3

http://s.sharesdk.cn/api/convert3.do

http://shouji.360tpcdn.com/140808/b669c90a340011f7bb52c731af4f432d/com.goodlogic.cutejellypets_4.apk

https://play.google.com/store/

http://media.admob.com/mraid/v1/mraid_app_interstitial.js

URLs incluidas en el código de aplicación que apuntan a una "apk"

Identificando amenzas en tu móvil

Leonardo Huertas Calle
CSA – Chief Security Ambassador at 11Paths
leonardo.huertas@11paths.com
@SamuraiBlanco