



Invasión zombie al mundo de Android

Jose Moruno Cadima

AndroidCamp - Octubre 2013

Índice

Contenido

- 1 Whoami**
- 2 Introducción**
- 3 Historia**
- 4 La infección Zombie**

Índice

Contenido

1 Whoami

2 Introducción

3 Historia

4 La infección Zombie

Whoami

Mi nombre es: Jose Moruno Cadima A.K.A Snifer.

- Consultor trabajo actualmente en Yanapti.
- Desarrollador en Python, Perl, Ruby.
- Analisis de Malware.
- Android Forensic.
- Integrante de Uremix, HackLab Cochabamba, Grampus Team.
- Mi pagina personal es: <http://sniferl4bs.com>

Whoami

Mi nombre es: Jose Moruno Cadima A.K.A Snifer.

- Consultor trabajo actualmente en Yanapti.
- Desarrollador en Python, Perl, Ruby.
- Analisis de Malware.
- Android Forensic.
- Integrante de Uremix, HackLab Cochabamba, Grampus Team.
- Mi pagina personal es: <http://sniferl4bs.com>

Whoami

Mi nombre es: Jose Moruno Cadima A.K.A Snifer.

- Consultor trabajo actualmente en Yanapti.
- Desarrollador en Python, Perl, Ruby.
- Análisis de Malware.
- Android Forensic.
- Integrante de Uremix, HackLab Cochabamba, Grampus Team.
- Mi página personal es: <http://sniferl4bs.com>

Whoami

Mi nombre es: Jose Moruno Cadima A.K.A Snifer.

- Consultor trabajo actualmente en Yanapti.
- Desarrollador en Python, Perl, Ruby.
- Análisis de Malware.
- Android Forensic.
- Integrante de Uremix, HackLab Cochabamba, Grampus Team.
- Mi página personal es: <http://sniferl4bs.com>

Whoami

Mi nombre es: Jose Moruno Cadima A.K.A Snifer.

- Consultor trabajo actualmente en Yanapti.
- Desarrollador en Python, Perl, Ruby.
- Análisis de Malware.
- Android Forensic.
- Integrante de Uremix, HackLab Cochabamba, Grampus Team.
- Mi página personal es: <http://sniferl4bs.com>

Whoami

Mi nombre es: Jose Moruno Cadima A.K.A Snifer.

- Consultor trabajo actualmente en Yanapti.
- Desarrollador en Python, Perl, Ruby.
- Análisis de Malware.
- Android Forensic.
- Integrante de Uremix, HackLab Cochabamba, Grampus Team.
- Mi página personal es: <http://sniferl4bs.com>

Índice

Contenido

1 Whoami

2 Introducción

3 Historia

4 La infección Zombie

Índice

Contenido

2 Introducción

- Snifer anda loco como que zombies
- Para quien va dirigida la charla
- Porque la charla

Introducción

Snifer anda loco como que zombies



Nuestro amigo es controlado...

Índice

Contenido

2 Introducción

- Snifer anda loco como que zombies
- Para quien va dirigida la charla
- Porque la charla

Introducción

Para quien va dirigida la charla

¿Que es Android?

Solo vine a ver,
que había en el
mARTadero :)



Introducción

Para quien va dirigida la charla



Introducción

Para quien va dirigida la charla



Índice

Contenido

2 Introducción

- Snifer anda loco como que zombies
- Para quien va dirigida la charla
- Porque la charla

Introducción

Porque la charla

- 1 Concientizar a un usuario normal.
- 2 No pidan permisos innecesarios.
- 3 Mostrar un poco de lo que me gusta.
- 4 Proteger nuestros datos personales.

Introducción

Porque la charla

- 1 Concientizar a un usuario normal.
- 2 No pidan permisos innecesarios.
- 3 Mostrar un poco de lo que me gusta.
- 4 Proteger nuestros datos personales.

Introducción

Porque la charla

- 1 Concientizar a un usuario normal.
- 2 No pidan permisos innecesarios.
- 3 Mostrar un poco de lo que me gusta.
- 4 Proteger nuestros datos personales.

Introducción

Porque la charla

- 1 Concientizar a un usuario normal.
- 2 No pidan permisos innecesarios.
- 3 Mostrar un poco de lo que me gusta.
- 4 Proteger nuestros datos personales.

Índice

Contenido

1 Whoami

2 Introducción

3 Historia

4 La infección Zombie

Historia

Trabajo en Apple y Microsoft

Andy Rubin llevaba desde 1989 hasta 2003 trabajando como ingeniero en telecomunicaciones y en el mundo de los teléfonos móviles. Android Inc

Cuando se creó el Market

Android 1.0 Apple Pie 22 de octubre de 2008.

Historia



Trabajo en Apple y Microsoft

Andy Rubin llevaba desde 1989 hasta 2003 trabajando como ingeniero en telecomunicaciones y en el mundo de los teléfonos móviles. Android Inc

Cuando se creó el Market

Android 1.0 Apple Pie 22 de octubre de 2008.

Historia

Andy es su nombre

El nombre del hombrecito verde es Andy.

Andy Rubin

"La misma plataforma, el exacto sistema operativo que construimos para cámaras, eso se convirtió en Android para teléfonos inteligentes".

Historia

Andy es su nombre

Es un software dañino cuyo objetivo es infiltrarse o dañar un equipo.

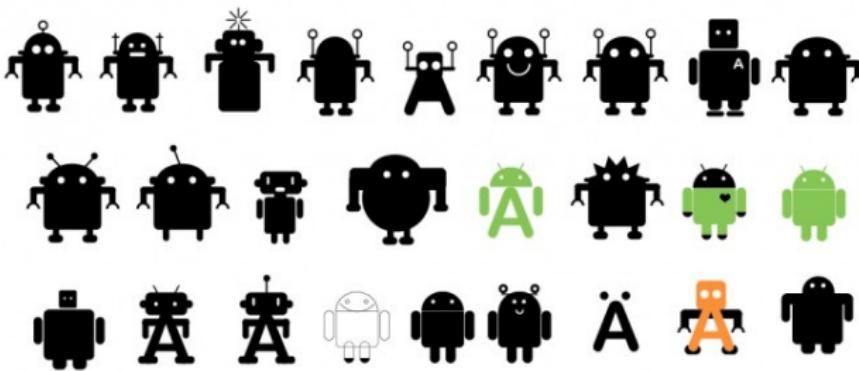


Historia



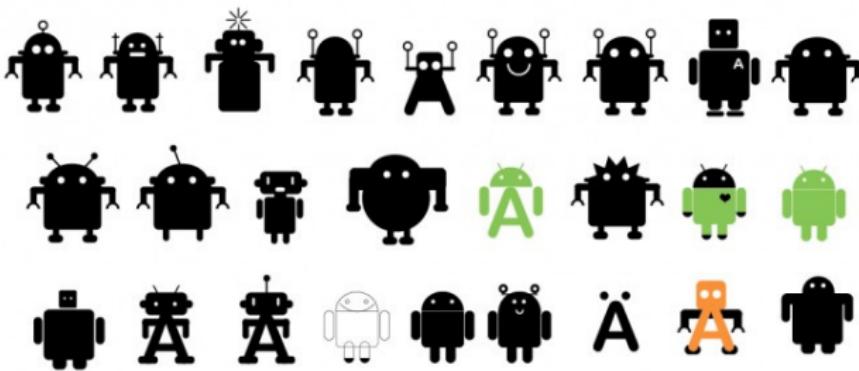
Historia

Los posibles Andy.



Historia

Los posibles Andy.



Índice

Contenido

- 1 Whoami
- 2 Introducción
- 3 Historia
- 4 La infección Zombie

Índice

Contenido

4 La infección Zombie

- Permisos innecesarios en aplicaciones
- El Play Store el foco de infección
- El mercado negro de las aplicaciones
- Cómo sobrevivir al apocalipsis
- Lo que hacemos hoy...

La infección Zombie

Permisos innecesarios en aplicaciones

Los culpables los desarrolladores....

- 1 El mal manejo de permisos por parte de los desarrolladores.
- 2 No pidan permisos innecesarios.
- 3 Malas prácticas de desarrollo.
- 4 Solicita todos los permisos así te evitas de problemas.

La infección Zombie

Permisos innecesarios en aplicaciones

Los culpables los desarrolladores....

- 1 El mal manejo de permisos por parte de los desarrolladores.
- 2 No pidan permisos innecesarios.
- 3 Malas prácticas de desarrollo.
- 4 Solicita todos los permisos así te evitas de problemas.

La infección Zombie

Permisos innecesarios en aplicaciones

Los culpables los desarrolladores....

- 1 El mal manejo de permisos por parte de los desarrolladores.
- 2 No pidan permisos innecesarios.
- 3 Malas prácticas de desarrollo.
- 4 Solicita todos los permisos así te evitas de problemas.

La infección Zombie

Permisos innecesarios en aplicaciones

Los culpables los desarrolladores....

- 1 El mal manejo de permisos por parte de los desarrolladores.
- 2 No pidan permisos innecesarios.
- 3 Malas prácticas de desarrollo.
- 4 Solicita todos los permisos así te evitas de problemas.

La infección Zombie

Permisos innecesarios en aplicaciones

Una aplicación solicita demasiados permisos para muestra unos botones.

Permisos de aplicaciones

Instanote - Add text to Photos necesita acceder a:

Llamadas de teléfono

Consultar la identidad y el estado del teléfono

Herramientas del sistema

Conectarse a redes WiFi y desconectarse

Memoria

Editar o borrar contenido de USB

Controles de hardware

Realizar fotografías y videos

Comunicación de red

Acceso completo a red

Ocultar

Herramientas de desarrollo

Probar acceso a memoria protegida

Herramientas del sistema

Instalar accesos directos

La infección Zombie

Permisos innecesarios en aplicaciones

Permisos de aplicaciones

Text Photo necesita acceder a:

Tu ubicación

Ubicación aproximada (basada en red),
ubicación exacta (GPS)

Llamadas de teléfono

Consultar la identidad y el estado del teléfono

Comunicación de red

Acceso completo a red

Memoria

Editar o borrar contenido de USB

Ver todo

ACEPTAR

La infección Zombie

Permisos innecesarios en aplicaciones

Permisos de aplicaciones

Photo Text Editor: Fun Camera necesita acceder a:

Tu información personal

Consultar tu historial y tus marcadores web, escribir en el historial y en los favoritos web

Llamadas de teléfono

Consultar la identidad y el estado del teléfono

Tu ubicación

Ubicación aproximada (basada en red)

Memoria

Editar o borrar contenido de USB

Controles de hardware

Realizar fotografías y vídeos

Comunicación de red

Acceso completo a red

Ver todo

ACEPTAR

Índice

Contenido

4 La infección Zombie

- Permisos innecesarios en aplicaciones
- El Play Store el foco de infección
- El mercado negro de las aplicaciones
- Cómo sobrevivir al apocalipsis
- Lo que hacemos hoy...

La infección Zombie

El Play Store el foco de infección

Play Store hasta 2012, no revisaba de forma alguna las aplicaciones que le enviaban los desarrolladores.

El protocolo de actuación de Google se limitaba a revisar la aplicación (y retirarla, si se daba el caso) en base al número de denuncias recibidas por parte de los usuarios.

Índice

Contenido

4 La infección Zombie

- Permisos innecesarios en aplicaciones
- El Play Store el foco de infección
- El mercado negro de las aplicaciones
- Cómo sobrevivir al apocalipsis
- Lo que hacemos hoy...

La infección Zombie

El mercado negro de las aplicaciones

¿Quienes tienen aplicaciones de pago en el móvil?

Legalmente compradas :)

¿De donde consiguen esas aplicaciones?

La infección Zombie

El mercado negro de las aplicaciones

¿Quienes tienen aplicaciones de pago en el móvil?

Legalmente compradas :)

¿De donde consiguen esas aplicaciones?

La infección Zombie

El mercado negro de las aplicaciones

¿Quienes tienen aplicaciones de pago en el móvil?

Legalmente compradas :)

¿De donde consiguen esas aplicaciones?

La infección Zombie

El mercado negro de las aplicaciones

Unofficial Android Marketplaces



Índice

Contenido

4 La infección Zombie

- Permisos innecesarios en aplicaciones
- El Play Store el foco de infección
- El mercado negro de las aplicaciones
- Como sobrevivir al apocalipsis
- Lo que hacemos hoy...

La infección Zombie

Como sobrevivir al apocalipsis



SAM SPRATT - GIZMODO

Índice

Contenido

4 La infección Zombie

- Permisos innecesarios en aplicaciones
- El Play Store el foco de infección
- El mercado negro de las aplicaciones
- Como sobrevivir al apocalipsis
- Lo que hacemos hoy...

La infección Zombie

Lo que hacemos hoy...

LOS ACTOS PRESENTES DERIVAN LA SITUACIÓN FUTURA.



Gracias por su atención



Twitter: @sniferl4bs
Skype: sniferl4bs

Jose Moruno Cadima

snifer@h-sec.org